

## *– Decalogo ABI Lab per le banche*

Sebbene il fenomeno del phishing sia un tipo di frode che agisce all'esterno del sistema bancario, alcuni accorgimenti possono essere ravvisati, in modo da ridurre per quanto possibile l'incidenza tra i propri clienti. In particolare può risultare opportuno quanto segue.

1. **Definire policy aziendali stringenti per il contatto del cliente via e-mail**; ad esempio, stabilire i processi autorizzativi e gli indirizzi di posta elettronica abilitati per l'invio di e-mail ai clienti, non utilizzare mai un indirizzo e-mail che non appartiene al dominio web della banca.
2. **Pubblicizzare ai dipendenti e ai clienti della banca le policy di utilizzo dell'e-mail**; in particolare, evidenziare che in nessun caso la banca chiederà ai clienti informazioni quali chiavi di accesso al servizio di home banking, codici di carte di pagamento o altre informazioni personali via e-mail. È opportuno inoltre diffondere le policy di utilizzo del contatto via e-mail della banca attraverso canali diversificati; ad esempio tramite spazi sul sito istituzionale, comunicazioni cartacee, messaggi in filiale,...
3. In caso di e-mail inviate ai clienti, **non inserire link a pagine interne del sito istituzionale o a siti esterni**, ma rimandare a comunicazioni che si trovano nella home page del sito, in modo che il cliente possa verificare l'autenticità della comunicazione, digitando manualmente l'indirizzo web della banca nella barra degli indirizzi del proprio browser.
4. **Aggiungere un ulteriore livello di autenticazione** (con password differenziata) per l'esecuzione di operazioni dispositive tramite il servizio di home banking. Si tratta di un ulteriore accorgimento in grado di limitare i danni prodotti da questo tipo di frode.
5. **Prevedere un processo di modifica / aggiornamento delle chiavi di accesso** al servizio di home banking su richiesta o necessità legata alla perdita della riservatezza di tali dati. Se non è possibile un'immediata modifica delle chiavi di accesso, è opportuno predisporre un servizio di blocco immediato delle chiavi stesse.
6. **Non utilizzare pop up per operazioni che richiedano interazione con l'utente**, in particolare modo per l'autenticazione e l'inserimento di dati. Il pop up di navigazione è la modalità principale con cui vengono condotte queste frodi e quindi può essere utilizzato come elemento di riconoscimento della frode da parte dell'utente.
7. Predisporre **strumenti di monitoraggio delle transazioni** dei propri conti online, in modo da evidenziare eventuali comportamenti anomali.
8. Predisporre un apposito **indirizzo e-mail ed eventualmente un numero telefonico cui i clienti possano rivolgersi in caso di sospetta frode**. Può inoltre essere utile costituire una raccolta delle segnalazioni pervenute.
9. **Dare informazione all'help desk clienti e al call centre** della banca affinché possa supportare la clientela su eventuali richieste di informazioni riguardanti questa tipologia di frode.
10. In caso di rilevazione di un attacco di phishing, informare la Polizia Postale e delle Comunicazioni.