

## Come proteggersi dal **PHISHING**

### – 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 un’*e-mail* contenente richieste di questo tipo, **non rispondete all’e-mail** stessa, ma informate subito la vostra banca tramite il *call centre* 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 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 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 centre* 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 anti-virus presente sul proprio computer.**
10. Internet è un po' come il mondo reale: come non darestes 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 alla vostra banca!**

## – 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 ridurne 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 particolar 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 *on-line*, 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.