

DECALOGO ANTIPHISHING DELL'ABI

Di seguito proponiamo il decalogo stilato dall'**ABI** per proteggersi dal Phishing:

1. diffidate di qualunque e-mail che richieda l'inserimento di dati riservati: **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; non riportano una data di scadenza per l'invio delle informazioni
3. nel caso in cui riceviate un messaggio contenente richieste di questo tipo, **non rispondete via e-mail**, 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 ad 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 far visualizzare un indirizzo diverso da quello nel quale realmente vi trovate
5. **diffidate inoltre di e-mail con indirizzi web molto lunghi**, contenenti caratteri inusuali
6. 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**
7. **diffidate se improvvisamente cambia la modalità con la quale vi viene chiesto di inserire i vostri codici di accesso** allo 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
8. **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 o l'emittente della carta
9. 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
10. Internet è un po' come il mondo reale: come non daresti 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**.