

I dieci consigli dell'ABI per l'home banking sicuro

Protezione, riservatezza e sicurezza. Le banche italiane rispondono efficacemente alle richieste dei clienti di poter accedere ai servizi bancari online, sia tramite Pc sia in mobilità, in modo facile, veloce e, soprattutto, sicuro. Con lo sviluppo delle nuove tecnologie e dell'economia digitale cresce l'impegno del mondo bancario nella lotta ai crimini informatici, attraverso presidi tecnologici, iniziative di formazione del personale e campagne di sensibilizzazione della clientela. Per questo motivo, ABI Lab, il centro di ricerca e innovazione per la Banca promosso dall'ABI, ha sintetizzato in 10 punti le principali regole da seguire per operare online in modo comodo e sicuro.

- ✓ Diffida di qualunque richiesta di dati relativi a carte di pagamento, chiavi di accesso all'home banking o altre informazioni personali ricevute su qualsiasi canale digitale (posta elettronica, sms, etc.). **La tua banca e qualunque altra Autorità non ti chiederanno mai queste informazioni**, anche in ragione di presunti motivi tecnici o di sicurezza.
- ✓ Per connetterti al sito della tua banca, scrivi direttamente l'indirizzo nella barra di navigazione. **Non cliccare su link presenti su e-mail e sms**, che potrebbero invece condurti su siti contraffatti, molto simili all'originale.
- ✓ **Verifica l'autenticità della connessione con la tua banca**, controllando con attenzione il nome del sito nella barra di navigazione. Se è presente, "clicca" due volte sull'icona del lucchetto (o della chiave) in basso a destra nella finestra di navigazione e verifica la correttezza dei dati che vengono visualizzati.
- ✓ Controlla regolarmente le movimentazioni del tuo conto corrente per assicurarti che le transazioni riportate siano quelle realmente effettuate e **utilizza eventuali strumenti di notifica delle operazioni svolte se messi a disposizione dalla tua banca**.
- ✓ **Se riscontri problemi o anomalie** nei servizi di home banking rivolgiti alla tua banca, che potrà darti informazioni utili.
- ✓ **Diffida di qualsiasi messaggio, anche se apparentemente autentico, ricevuto tramite e-mail, sms, social network, etc. che ti invita a scaricare documenti o programmi** in allegato. Potrebbero contenere dei malware che si installano sul tuo pc.
- ✓ **Installa e mantieni aggiornati software di protezione** (antivirus e antispyware), ed effettua delle scansioni periodiche del tuo hard disk.
- ✓ **Aggiorna costantemente sistema operativo e applicativi del computer**, installando solo gli aggiornamenti ufficiali disponibili sui siti web delle aziende produttrici.
- ✓ Durante la navigazione in internet, **installa solo programmi di cui puoi verificare la provenienza**.
- ✓ **Fai attenzione a eventuali peggioramenti delle prestazioni generali** (rallentamenti, apertura di finestre non richieste, ecc.) o a qualsiasi modifica improvvisa delle impostazioni di sistema, che possono indicare infezioni sospette.