IN SINTESI

Ricorda: per operare online, in sicurezza, è importante seguire poche semplici regole:

- **non comunicare a nessuno i codici di accesso** e scegliere password/PIN difficili da indovinare, che non facciano riferimento alla vita personale e modificarle periodicamente (almeno una volta ogni 6 mesi);
- alla fine delle tue transazioni, prima di uscire dal tuo sito di internet banking, **effettua il logout;**
- **controlla l'URL** del sito in cui ti trovi: controlla che l'indirizzo inizi con "https" e che ci sia il lucchetto con una zona verde;
- **installa e tieni sempre aggiornato l'anti-virus** su tutti i dispositivi che usi per accedere all'home banking;
- **attiva i servizi di notifica dell'accesso e delle disposizioni**, comunicando alla banca l'indirizzo e-mail e/o il cellulare tramite l'apposita funzione di Nowbanking. In generale, controlla periodicamente i movimenti registrati sui conti e le spese delle carte.
- **attenzione ai social network e ai software di comunicazione**: i social network non sono solo sono ottimi strumenti per tenersi in contatto e condividere con amici, familiari, ma sono anche uno strumento straordinario per chiunque voglia raccogliere informazioni senza troppi sforzi. Pertanto:
  - usare le impostazioni di configurazione per proteggere il profilo: "Quale gruppo di amici sarà in grado di accedere a quali informazioni nel mio profilo?"
  - non comunicare informazioni sensibili sul proprio profilo; non dimenticare che tutti i contenuti condivisi sui social possono fornire informazioni per attacchi di spear phishing, furto di identità e altri tipo di violazione
  - imposta i le opzioni di privacy per proteggere i dati e le foto condivise
  - non condividere notizie prima di averle verificate
  - non usare la stessa password per account social e-mail e internet banking.
- **privilegia l'uso di dispositivi personali** e tieni aggiornato il sistema operativo e il browser;
- se utilizzi un computer condiviso, possibilmente non visitare un sito che richiede di fornire dati personali e ricordati di ripulire la cronologia del browser al termine dell'utilizzo;
- non « abboccare» al phishing: non cliccare mai su link e non scaricare allegati contenuti in e-mail o sms sospetti. Ricorda che la banca non chiede mai codici di accesso o altre informazioni personali mai via e-mail, telefono o sms;
- non comunicare il tuo indirizzo di posta principale sui siti commerciali e utilizza un altro indirizzo per offerte promozionali e acquisti online