Conto online: 10 mosse per proteggersi dalle truffe

16 Settembre 2020

Temete che la sicurezza del vostro conto corrente online possa essere messa a repentaglio? Ecco alcuni consigli preziosi: innanzitutto, è bene sapere che le informazioni e gli strumenti con cui accediamo ai servizi della banca (password, codici, carte, ecc…) sono strettamente personali e vanno custoditi con cura. E' bene poi tenere presente che per darci informazioni la banca può contattarci telefonicamente, via e-mail o sms, ma non ci chiederà mai di fornirle direttamente i nostri codici di accesso ai servizi quando ci contatta.

Ecco poi 10 mosse per proteggersi dalle truffe:

1. **controlliamo regolarmente e frequentemente gli estratti conto** dei nostri rapporti bancari. In questo modo possiamo assicurarci che le operazioni riportate siano quelle realmente effettuate.
2. Nei casi in cui riscontriamo anomalie nei conti riteniamo di essere stati vittime di una frode, **rivolgiamoci immediatamente alla banca**.
3. A tale scopo, **teniamo sempre a portata di mano i numeri di riferimento della banca**, come ad esempio il numero verde del call center, che possiamo chiamare sia

da telefono fisso che da cellulare.

4. **Avvaliamoci** dei **servizi di "notifica movimenti"** offerti dalle banche. In questo modo, ogni volta che effettuiamo operazioni online o usiamo il bancomat e la carta di credito la banca ci avvisa praticamente in tempo reale attraverso SMS o e-mail dei movimenti effettuati. Questo è un buon mezzo per accertarci che nessuno effettui operazioni al nostro posto.
5. **Installiamo adeguati software di protezione**(anti-virus e antispyware) sui dispositivi che utilizziamo per accedere all'Internet Banking e ricordiamoci di tenerli sempre aggiornati.
6. Se il nostro dispositivo (es. computer) è particolarmente lento o "si comporta" in modo strano **avviamo** una **scansione antivirus**: potremmo essere stati contagiati. Nel momento in cui accediamo alla pagina del nostro conto online, **controlliamo che non ci siano anomalie** nel momento in cui ci vengono richiesti codici o password di accesso.
7. **Modifichiamo** con una certa frequenza **le password** di accesso al servizio di internet banking.
8. Quando entriamo in un social network, **facciamo attenzione a non rendere pubbliche le informazioni più "sensibili"** che ci riguardano.
9. **Non rendiamo pubblici indirizzi, password o codici** e valutiamo con attenzione le richieste di dati personali da parte di chi non conosciamo, soprattutto quelle connesse a offerte di lavoro, alla proposta di "favolosi" investimenti o alla vincita di un premio "certo".
10. **Teniamo sempre aggiornate le informazioni personali comunicate alla banca**: costituiscono gli elementi di riconoscimento per l'accesso ai servizi che abbiamo sottoscritto.

HAI BISOGNO DI AIUTO? CONTATTACI ALLO SPORTELLO BANCHE

VUOI LEGGERE ALTRI CONSIGLI IN TEMA DI EDUCAZIONE FINANZIARIA? VISITA IL NOSTRO SITO informatiperdecidere.consumatori.it

Autore: Lorenzo Cargnelutti
Data: 23 novembre 2016
Aggiornamento: 20 agosto 2020