

Sicurezza informatica

Gentile Cliente,

Banca Consulia è da sempre impegnata nel tutelare la sicurezza informatica dei propri Clienti e, per aiutarti a proteggere i Tuoi dati, elenchiamo di seguito alcuni utili suggerimenti.

Codici personali

I codici personali servono per identificarti quando accedi alle Aree Clienti. Sono strettamente personali e non devono in alcun modo essere comunicati a terze persone.

Non trascriverli in modo evidente su documenti che possano essere smarriti o che possano essere letti da terzi.

Non memorizzare i Tuoi codici segreti su pc, smartphone o tablet.

Utilizza i codici personali solo sul sito di Banca Consulia: nessun dipendente, consulente finanziario Ti richiederà mai i codici personali, verbalmente o in forma scritta.

Ti consigliamo di cambiare ciclicamente la password di accesso.

Strong Authentication e Servizi SMS

Per accedere al Servizio internet banking MiTO ci si può collegare tramite il sito MiTO Cabel all'indirizzo <https://www.mito.cabel.it/Mito7>, tramite il sito di Banca Consulia all'indirizzo <https://www.bancaconsulia.it> o tramite l'APP MiTO Mobile, scaricabile da Google Play Store o Apple Store.

Ogni disposizione inserita dovrà essere confermata tramite il codice OTP (one time password) che sarà ogni volta diverso. I canali di ricezione del codice OTP potranno essere l'app VIP ACCESS oppure un SMS. Tutte le informazioni relative al cosiddetto sistema di Strong Authentication sono disponibili sul sito di Banca Consulia, sezione Trasparenza, settore Altri documenti.

Per le disposizioni effettuate con MiTO tramite App MiTO Mobile, la conferma avverrà inserendo il PIN, ricevuto tramite SMS al numero di cellulare primario indicato dal cliente, al momento dell'emissione dell'utenza e che sarà stato personalizzato al primo accesso.

Controlla periodicamente i movimenti del Tuo conto in modo da individuare eventuali addebiti fraudolenti.

Quando vuoi terminare la sessione clicca sempre sul tasto LOGOFF/ LOGOUT/ ESCI per chiudere correttamente la pagina internet e per maggiore sicurezza chiudi anche il browser.

Accedi sempre digitando direttamente l'indirizzo e non utilizzare mai i link riportati in e-mail e in popup o i link salvati tra i preferiti del browser.

Evita il salvataggio automatico delle password sul browser.

Frodi Informatiche

Attualmente in circolazione ci sono diverse forme di frodi informatiche.

Oltre ai messaggi e-mail inviati a malcapitati utenti, vengono utilizzate pagine web apparentemente simili, per esempio, al sito di Banca Consulia, per catturare in modo fraudolento codici di accesso ed eventuali altre informazioni, con l'invito a partecipare a sondaggi o recensioni. Ricorda che i sondaggi non devono richiedere l'inserimento di dati riservati come codici di accesso e non cliccare su link presenti in e-mail sospette perché potrebbero indirizzarti a siti contraffatti ma molto simili all'originale.

Verifica che la sessione sia protetta e che quindi nell'indirizzo della barra del browser compaia <https://> e non solo [http](http://) come in alcuni siti di truffatori.

- ✓ Ti forniamo alcune indicazioni per riconoscere le e-mail sospette: e-mail che non contengono "in chiaro" nome e cognome del destinatario in quanto inviate a molti utenti diversi;
- ✓ e-mail prive del link della banca www.bancaconsulia.it;
- ✓ e-mail che richiedono di indicare i Tuoi dati personali di accesso.

Infine, evita di scaricare screen saver, vignette animate da siti web sconosciuti o programmi apparentemente protetti poiché potresti scaricare involontariamente sul tuo pc software *keylogger* che registrano, all'insaputa dell'utente, quanto digitato sulla tastiera del computer: in questo modo potrebbero essere copiati anche dati riservati.

Se temi di aver fornito dati riservati o di aver utilizzato pagine web non sicure controlla che non siano state effettuate operazioni non autorizzate sul Tuo conto;

contatta il Tuo Financial Advisor per segnalare la possibilità di una frode oppure contatta direttamente l'Help Desk al numero 800.519.155 per il blocco dell'utenza (lun-ven 07,00-22,30).

In caso di operazioni presenti in conto corrente non disposte da Te è necessario sporgere denuncia presso un'autorità di pubblica sicurezza e inviare alla banca la copia della denuncia e la dichiarazione per disconoscere le operazioni disposte ma non riconosciute