Sicurezza informatica

Gentile Cliente,

Finint Private Bank 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, tablet su file non crittografati.

Utilizza i codici personali solo sul sito di Finint Private Bank: 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 di Finint Private Bank all'indirizzo https://www.finintprivatebank.com o tramite l'APP Mobile Finint Private Bank 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 Mobile Finint Private Bank oppure un SMS. Tutte le informazioni relative al cosiddetto sistema di Strong Authentication sono disponibili sul sito di Finint Private Bank, sezione Trasparenza, settore Altri documenti.

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.

Notifiche push

È la funzione che consente di confermare tramite smartphone le disposizioni inserite da home banking MITO, senza necessità di digitare il codice. Per attivare la funzione è necessario accedere alle impostazioni generali del proprio smartphone e autorizzare l'APP Finint Private Bank all'invio di notifiche.

La Notifica Push è valida per una singola operazione.

Frodi Informatiche

Attualmente in circolazione ci sono diverse forme di frodi informatiche.

Phishing

È un tipo di frode che consiste nel tentativo di carpire informazioni personali dei clienti (es. i codici segreti per accedere ai servizi bancari), tramite l'invio di messaggi contraffatti (tramite e-mail, SMS e whatspp) apparentemente provenienti da soggetti affidabili (es. la Banca).

Tenere sempre aggiornato l'antivirus del computer e di ogni dispositivo usato per aprire e-mail e navigare online.

Fare sempre attenzione ai dettagli delle e-mail, quali ad esempio l'indirizzo del mittente (confrontandolo con quello delle comunicazioni ufficiali).

Fare molta attenzione alla grammatica ed all'ortografia della comunicazione.

Non aprire mai allegati o link presenti all'interno di e-mail inaspettate, sospette o che paiono contraffatte.

In caso di dubbi, si consiglia comunque di contattare sempre la propria Banca o il proprio Financial Advisor

Crimeware

Si tratta di una tipologia di criminalità informatica perpetrata mediante l'infezione dei dispositivi degli utenti (PC, tablet, smartphone) per mezzo di virus informatici e software "malevoli" (malware) al fine, ad esempio, di eseguire furti di identità (sottrazione di informazioni personali, confidenziali, sensibili) e/o accedere fraudolentemente agli account dell'utente (es. bancari) con lo scopo di eseguire operazioni o transazioni fraudolente.

Installare sui propri dispositivi (PC, smartphone, tablet) un antivirus, mantenendolo sempre aggiornato.

Aggiornare costantemente il sistema operativo e gli applicativi in uso.

Effettuare spesso la pulizia dei file temporanei (cache e cookies).

Digitare manualmente l'indirizzo della banca nella barra degli indirizzi e verificare, una volta collegato, di trovarsi effettivamente sul sito di Finint Private Bank. Controllare che nella barra degli indirizzi sia presente l'indirizzo corretto e che i dati richiesti nella pagina non siano diversi dal solito.

Scaricare solo versioni ufficiali dei software da siti sicuri e Store/Appstore ufficiali.

Quando si naviga in internet non cliccare su link sospetti, pop-up o finestre di dialogo.

FININT PRIVATE BANK

Truffe d'investimento

Le più comuni truffe d'investimento riguardano opportunità insolitamente redditizie, generalmente sulle criptovalute o mercati esteri. Si ricorda di non confidare in chi promette grandi e immediati guadagni a fronte di investimenti minimi.

Non fornite mai a queste persone i codici di accesso alla banca o i dati delle carte di credito; allo stesso modo si raccomanda di non consentire loro di accedere in remoto al proprio computer/smartphone per operare al posto vostro sul conto corrente.

Chi chiama generalmente si pone in modo insistente e sottolinea come l'offerta sia limitata nel tempo.

Viene posto l'accento sull'unicità della proposta e sull'importanza di agire velocemente.

Nel caso si decidesse di investire su piattaforme finanziarie, si raccomanda di verificare sempre l'affidabilità e la credibilità della piattaforma, in particolare che sia registrata alla CONSOB.

Infine, evita di scaricare screen saver, vignette animate da siti web sconosciuti o programmi apparentemente protetti poichè 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