SÜDTIROL BANK

Guida alla sicurezza dei dati

LA SICUREZZA DEI DATI

La sicurezza e la riservatezza dei dati del Cliente sono pilastri fondamentali delle attività di Südtirol Bank (la "Banca").
Per questo motivo, vengono adottate molteplici misure atte a garantire la protezione dei dati dei nostri Clienti.
Anche il Cliente, tuttavia, in qualità di utente finale di sistemi informatici, ricopre un ruolo importante nel fronteggiare i rischi derivanti da frodi online e accessi non autorizzati.
Qui di seguito si riporta **una serie di linee guida che la aiuteranno a proteggersi e a comprendere i rischi e i comportamenti da adottare per fronteggiare le minacce.**

PROTEGGERSI DAL PISHING

Il pishing è una delle tipologie di frode informatica più comuni. Essa avviene quando si riceve posta elettronica che simula le comunicazioni ufficiali di una banca o di un servizio di pagamento e invita il destinatario a rilasciare informazioni riservate per impiegarle poi illegalmente. Di solito, le email contengono un link a un sito internet simile a quello originale frequentemente utilizzato dall'utente che viene invitato a inserire i dati relativi al proprio conto. Spesso la richiesta è motivata da guasti ai sistemi informatici della banca e all'utente viene richiesta una conferma del proprio nome utente e della password di accesso.

Alcune linee guida per proteggersi
È opportuno che:
- presti attenzione quando riceve un'email da mittenti sconosciuti, specie se presentano allegati (potrebbero contenere virus). La posta elettronica che giunge da indirizzi sospetti e richiede di seguire link anomali va trattata con estrema attenzione;
- quando riceve un messaggio della Banca, verifichi che l'indirizzo email sia coerente con l'indirizzo del sito web della Banca. Il dominio deve essere il medesimo: *……..@suedtirolbank.eu;*
- ponga attenzione ai messaggi che iniziano con un saluto generico (come, per esempio, "caro cliente"). La Banca normalmente si riferirà a lei nelle proprie comunicazioni utilizzando il suo nome;
- ponga attenzione ai messaggi che le richiedono informazioni personali, quali: utente, password o dettagli del conto (la Banca non lo farebbe mai, perché ne è già a conoscenza);
- acceda ai siti della Banca o ai siti dei sistemi di pagamento online solo direttamente dalla barra degli indirizzi, anziché seguendo link esterni. Cliccare sul link che viene proposto in una email sospetta è una pratica potenzialmente pericolosa.

PROTEGGERE IL PROPRIO COMPUTER

Il suo computer potrebbe essere al centro di attacchi fraudolenti, mirati ad infettarlo con un c. d. "software malevole" (o *"malware").* Una delle conseguenze di un attacco potrebbe essere la perdita delle informazioni conservate sul PC (documenti, dati, foto) e/o il furto di dati. Per questo è importante proteggere il PC con adeguati programmi antivirus e firewall.

Alcune linee guida per proteggersi
È opportuno che:
- mantenga aggiornato il sistema operativo del suo PC;
- mantenga aggiornato il suo browser per navigare in internet;

- protegga il PC con l'installazione di un programma antivirus e abbia cura di aggiornarlo periodicamente;
- installi un firewall;
- quando naviga in Internet, eviti di scaricare programmi o applicazioni che provengono da siti internet sospetti;
- non apra email sospette, soprattutto se presentano un allegato;
- stia attento quando condivide file su Internet: ciò la espone a rischi di virus e intrusioni dall'esterno.

PROTEGGERE I CODICI DI ACCESSO

PC, smartphone e tablet fanno ormai parte della nostra vita quotidiana: accediamo alla posta elettronica, accediamo online ai nostri conti in banca, effettuiamo pagamenti tramite i servizi di internet banking, facciamo acquisti online. E' fondamentale quindi proteggere le credenziali di accesso e la password.

Alcune linee guida per proteggersi
È opportuno che:
- vari spesso la sua password di accesso;
- scelga una password "forte", di difficile intuizione;
- conservi i suoi codici con la massima riservatezza;
- non salvi i suoi codici sul PC o sul cellulare;
- non usi le funzionalità del browser Internet per memorizzare i codici di accesso (PIN, password), ma li inserisca manualmente ogni volta che si connette;
- controlli regolarmente gli estratti conto dei suoi conti e dei servizi di pagamento, per essere sicuro che le transazioni visualizzate corrispondano esattamente a quelle realmente effettuate;
- quando termina le operazioni di internet banking o di altri servizi online, effettui la disconnessione mediante la funzionalità del log-out.

FARE ATTENZIONE AI DISPOSITIVI MOBILI

Oggi - grazie a Internet e all'utilizzo di smartphone, PC mobile e tablet – siamo in grado di svolgere attività bancarie e pagamenti ovunque siamo. Questo però rappresenta un altro livello di rischio: si potrebbe dimenticare, perdere o farsi sottrare i dispositivi mobili e correre il rischio di un abuso dei dati e degli accessi online. Per questo motivo è importante adottare tutte le misure necessarie per evitare qualsiasi sorpresa.
Anche lo smaltimento, la donazione o la vendita dei dispositivi non più utilizzati deve essere gestito correttamente per evitare che i dati conservati sul dispositivo o PC (email, dati di accesso, documenti, contratti) vengano a conoscenza di terzi.

COSA FARE IN CASO DI PROBLEMI

Se Lei ritiene che, in qualsiasi modo, sia stata compromessa la sicurezza dei dati relativi ai rapporti in essere con la nostra Banca, la invitiamo a contattare tempestivamente il Consulente Finanziario di riferimento oppure a scrivere direttamente alla Banca, all'indirizzo info@suedtirolbank.eu.