I consigli per un uso sicuro dei servizi digitali

L'Internet Banking è a oggi tra i servizi web maggiormente utilizzati da privati e imprese, con una crescente operatività online. Però, a fronte dei benefici dell'innovazione tecnologica e del boom di utilizzatori del canale online per l'accesso ai servizi bancari, è importante tenere conto dei rischi ad esso connessi.

Ecco perché di seguito pubblichiamo alcune indicazioni finalizzate alla protezione delle postazioni dalle quali viene svolta l'attività di Internet Banking (PC Utente). Sono best practice di carattere generale che ogni individuo che svolge operazioni bancarie online dovrebbe mettere in pratica per ridurre il rischio che le proprie credenziali vengano sottratte o violate.

- Custodire con la massima cura e non cedere ad altri il codice utente, la password, il PIN, la password dispositiva o il Token OTP
- Modificare periodicamente la password di accesso. Per la scelta della password non utilizzare la stessa che consente l'accesso alla tua posta elettronica oppure ad altri servizi web.
- Non inserire i propri codici personali nei siti internet raggiunti tramite click su link presenti nelle email o in qualsiasi altro sito diverso da quello di Conto Twist
- Accedere ai servizi Home Banking direttamente dal sito della Banca, digitando l'indirizzo internet www.contotwist.it nella barra di navigazione. Se invece si utilizzano dispositivi mobile (smartphone, tablet, ect), scaricare esclusivamente le applicazioni ufficiali di Conto Twist.
- Evitare di collegarsi a reti sconosciute
- Controllare regolarmente i propri estratti conto
- Attivare, ove possibile, i servizi di notifica via SMS o Email relativi a prelievi, pagamenti ed operazioni dispositive effettuate sui servizi di Home Banking
- Scaricare e utilizzare sul proprio computer solo programmi affidabili e ufficiali, evitando di installare codice malevolo
- Difendere da virus e spyware i PC dai quali si effettuano le operazioni di Internet Banking, installando e mantenendo aggiornati opportuni software di protezione (anti-virus, anti-spyware, anti-spam, sistemi di protezione del browser etc)
- Proteggere il traffico in entrata e in uscita dai PC mediante l'installazione di opportuni programmi di filtraggio del flusso di dati (firewall) e non disabilitare le impostazioni di protezione configurate
- Aggiornare costantemente il sistema operativo e gli applicativi del PC mediante l'installazione delle cosiddette patch ("toppe" di protezione)
- Profilare e controllare la navigazione in internet in base alle specifiche esigenze personali, limitando la navigazione sul web (anche ad esempio con ricorso a white list)
- Configurare i propri dispositivi mobile attivando le idonee impostazioni di sicurezza quali ad esempio il blocco automatico in caso di mancato utilizzo oppure il riconoscimento attraverso fattori biometrici (Face ID o Finger Print).

Qualora non siano state implementate le procedure sopra descritte è meglio svolgere tutte le movimentazioni bancarie da un dispositivo personale con posta elettronica e navigazioni controllate e sicure.

Diffida da qualunque richiesta di dati relativi a carte di pagamento, chiavi d'accesso all'Internet Banking o altre informazioni sensibili; di qualsiasi messaggio (proveniente da posta elettronica, siti web, social network, contatti di instant messaging, chat o peer-to-peer) che rivolga l'invito a scaricare programmi o documenti di cui si ignora la provenienza. Per contrastare fenomeni, esterni ed indesiderati, informiamo che Banca Valsabbina, o nessuna società per essa, non chiederà in alcun modo:

- dati personali o verifiche sui codici di accesso tramite email, a meno che sia richiesta specifica assistenza da parte dell'utente stesso;
- l'inserimento del codici di accesso su pagine web diverse da quelle normalmente utilizzate dalla banca in modalità protetta con protocollo HTTPS.