Gruppo UBI Banca

La sicurezza del tuo Home Banking

Gruppo UBI Banca

La sicurezza del tuo Home Banking Virty

Il nostro servizio di Home Banking Virty è sicuro anche grazie ai seguenti strumenti

- **Protezione della trasmissione dei dati**

La trasmissione dei dati con il nostro Home Banking è protetta attraverso il sistema di crittografia SSL a 128 bit (compatibile AES 256 bit), il protocollo standard che consente di stabilire un canale di comunicazione sicuro per impedire l'intercettazione di informazioni riservate che viaggiano sulla rete Internet. Per assicurarti che la protezione sia attiva verifica che nella parte inferiore della finestra del browser Internet Explorer sia sempre presente il lucchetto chiuso alternativamente l'icona colorata nella parte sinistra della barra indirizzo se hai Firefox.

- **I codici di accesso**

DISPOSITIVO OTP

Il servizio utilizza un sistema combinato di password statiche (il Codice Utente e la Password scelti da te durante il primo accesso) e per aumentare il livello di sicurezza, chiede la password dinamica, prodotta dal dispositivo OTP. Il dispositivo OTP genera ogni 60 secondi una password "usa e getta" per accedere al servizio e confermare le operazioni dispositive.

- **Gli avvisi via SMS**

Puoi attivare il servizio di Sms Alert. Un SMS ti avviserà inviandoti un messaggio sul tuo cellulare per ogni accesso al tuo Virty e per ogni eventuale disposizione effettuata.

- **La durata massima della sessione**

Per tutelare maggiormente la tua sicurezza il nostro Home Banking Virty prevede un tempo massimo di utilizzo di circa 20 minuti, passato il quale, il sistema interrompe automaticamente la connessione

Gruppo UBI Banca

Riconoscere le frodi online

Il nostro servizio di Home Banking è sicuro ma occorre anche la tua collaborazione per avere un PC sempre protetto e per aumentare il livello di sicurezza

- **Ecco alcune regole che possono aiutarti:**

1) Fare sempre attenzione alle e-mail false

Stiamo parlando di **PHISHING**, un tentativo di truffa che **non viola** i sistemi di Home Banking (che garantiscono comunque la massima sicurezza), ma tenta di ingannare gli utenti facendosi consegnare i codici segreti. Quindi è **assolutamente necessario non fornire i propri codici dispositivi** se non per confermare le disposizioni che si stanno effettuando consapevolmente dal proprio Home Banking.

Come si verifica:

L'utente riceve una e-mail simile a quella della banca presso cui è cliente in cui viene invitato a collegarsi ad un link; cliccando si accede ad un sito simile solo nella grafica a quello della Banca. Nel "falso sito" viene richiesto l'inserimento dei propri codici segreti. Seguendo le istruzioni riportate, il cliente si collega al sito e trasmette lui stesso ai "truffatori" le proprie informazioni personali.

Come tutelarsi:

- **Non inserire mai i tuoi dati personali all'interno di e-mail**. Nuova Banca Etruria non ha mai richiesto i tuoi dati tramite e-mail, né lo farà mai.
- **Cerca di identificare le e-mail false**: solitamente non sono personalizzate, dichiarano motivazioni di invio non precise, come ad esempio la scadenza o lo smarrimento dei codici, fantomatici problemi tecnici o di sicurezza. Spesso minacciano la sospensione del servizio in caso di mancata risposta.
- **Non cliccare su link e non aprire file allegati**: i siti web "truffa" non vanno mai visitati ed i file allegati non devono mai essere scaricati sul proprio PC.
- **Segnala di aver ricevuto una e-mail sospetta**: nel caso in cui ricevi una e-mail e non sei completamente sicuro della sua autenticità, puoi chiamare la tua agenzia o il Numero Verde **800.311.346** per saperne di più.

2) Controllare la sicurezza di ogni sito prima di fornire dati riservati

Prima di inserire in un sito web i propri codici/password o numeri di carte di credito/debito, occorre sempre verificare che la trasmissione dei dati sia "sicura" e che il sito web sia autentico. In particolare occorre:

- Verificare sempre la presenza del prefisso "**https://**" nell'indirizzo web.
- Accertarsi che sia presente:

- l'icona "**lucchetto chiuso**" nella barra di stato del browser se hai Internet Explorer
- l'icona colorata nella parte sinistra della barra indirizzo se hai Firefox

- Fare doppio click sull'icona per controllare che sia attivo il **protocollo SSL 128bit** che protegge la trasmissioni dei dati.

I codici segreti di identificazione del tuo Home Banking non devono mai essere "salvati" nella memoria del browser o del Personal Computer.

Per disabilitare e cancellare le password già salvate:
- se hai Internet Explorer:
    - clicca sulla funzione Opzioni Internet nel menù Strumenti;
    - nella cartella Contenuto, clicca sul tasto Completamento Automatico;
    - elimina la selezione da Nome Utente e Password sui moduli;
    - cancella i dati precedentemente memorizzati cliccando sui tasti Cancella Moduli e Cancella Password;
    - completa l'operazione cliccando il tasto OK su tutte le finestre precedentemente aperte.
- se hai Firefox:
    - clicca sul menù Strumenti ed attiva Opzioni;
    - clicca quindi sulle voci Privacy, Impostazioni e seleziona Password Salvate;
    - premi OK per chiudere la finestra di opzioni.

4) Proteggere il computer con AntiVirus e dispositivi di filtraggio

L'Antivirus è un ottimo strumento per stare al sicuro da tentativi di intrusione e virus. Ricordati di effettuare nel tempo i vari aggiornamenti generalmente segnalati online dal produttore anche nel proprio sito. Inoltre può essere utile utilizzare programmi per la gestione della posta elettronica perché sono in grado di attenuare i rischi filtrando molte e-mail sospette. Un'ulteriore protezione contro gli hacker, facilmente scaricabile da Internet o acquistabile, è rappresentata dai dispositivi Firewall, che tengono sotto controllo ciò che entra e ciò che esce dal PC, proprio come dei "buttafuori" digitali. .

5) Selezionare la condivisione dei file su Internet

Condividere file su Internet (con i software per scaricare mp3, video, etc.) significa lasciare una "porta aperta" e quindi permettere l'accesso a "ospiti" indesiderati. Particolari software denominati Spyware, possono avere facile accesso e "catturare" via Internet informazioni personali a tua insaputa. Evita quindi di condividere file se vuoi aumentare la sicurezza.

6) Aggiorna spesso il Sistema Operativo

Le aziende produttrici dei Sistemi Operativi rendono disponibili gli aggiornamenti, scaricabili gratuitamente online. Si tratta delle cosiddette Patch, che incrementano, tra l'altro, la sicurezza dei programmi.

Gruppo UBI Banca

I dieci consigli dell'ABI per l'home banking sicuro

Diffida di qualsiasi messaggio, anche se apparentemente autentico, ricevuto tramite e-mail, sms, social network, etc. che ti invita a scaricare documenti o programmi in allegato. Potrebbero contenere dei malware che si installano sul tuo pc.

Diffida di qualunque richiesta di dati relativi a carte di pagamento, chiavi di accesso all'home banking o altre informazioni personali ricevute su qualsiasi canale digitale (posta elettronica, sms, etc.). **La tua banca e qualunque altra Autorità non ti chiederanno mai queste informazioni**, anche in ragione di presunti motivi tecnici o di sicurezza.

Per connetterti al sito della tua banca, scrivi direttamente l'indirizzo nella barra di navigazione. **Non cliccare su link presenti su e-mail e sms**, che potrebbero invece condurti su siti contraffatti, molto simili all'originale.

Controlla regolarmente le movimentazioni del tuo conto corrente per assicurarti che le transazioni riportate siano quelle realmente effettuate e **utilizza eventuali strumenti di notifica delle operazioni svolte se messi a disposizione dalla tua banca**.
Verifica l'autenticità della connessione con la tua banca, controllando con attenzione il nome del sito nella barra di navigazione. Se è presente, "clicca" due volte sull'icona del lucchetto (o della chiave) in basso a destra nella finestra di navigazione e verifica la correttezza dei dati che vengono visualizzati.

Durante la navigazione in internet, **installa solo programmi di cui puoi verificare la provenienza**.
Installa e mantieni aggiornati software di protezione (antivirus e antispyware), ed effettua delle scansioni periodiche del tuo hard disk.

Aggiorna costantemente sistema operativo e applicativi del computer, installando solo gli aggiornamenti ufficiali disponibili sui siti web delle aziende produttrici.

Fai attenzione a eventuali peggioramenti delle prestazioni generali (rallentamenti, apertura di finestre non richieste, ecc.) o a qualsiasi modifica improvvisa delle impostazioni di sistema, che possono indicare infezioni sospette.

Se riscontri problemi o anomalie nei servizi di home banking rivolgiti alla tua banca, che potrà darti informazioni utili.