GUIDA ALLA SICUREZZA IN INTERNET

Gentile Cliente,

Le riportiamo di seguito alcuni utili consigli per navigare in internet con la massima sicurezza.

Anzitutto, accedendo ai link internet sotto riportato è possibile verificare gratuitamente se il proprio computer è protetto o se è stato infettato da qualche virus:

http://security.symantec.com

In generale, per operare in assoluta tranquillità con i sistemi di INTERNET BANKING è necessario utilizzare il computer in modo corretto, evitando comportamenti a rischio e proteggendolo con gli strumenti hardware e software più opportuni.

Ecco perché esistono **6 REGOLE GENERALI** a cui gli utilizzatori devono attenersi:

- **Fare attenzione alle email false**
- **Controllare la sicurezza del sito prima di fornire dati riservati**
- **Evitare il "salvataggio automatico" delle password sul browser**
- **Proteggere il computer con AntiVirus e dispositivi di filtraggio**
- **Non condividere file su Internet**
- **Aggiornare spesso il Sistema Operativo**

Nascono dalla nostra esperienza e dalle ultime novità nel campo della sicurezza online. Adottale per la tua azienda ed **eviterai** qualsiasi tentativo di **truffa**, ma anche inutili perdite di tempo.

1) FARE ATTENZIONE ALLE EMAIL FALSE

Si chiama "**phishing**". E' una truffa che si è verificata soprattutto in nord Europa e in America, sebbene ultimamente siano arrivate diverse segnalazioni anche in Italia.

L'utente riceve un'email simile a quella della sua banca e **viene invitato a collegarsi a un link**. L'indirizzo sembra corretto, ma cliccando si accede a un sito che non ha nulla a che fare con quello che si pensava di visitare,

nonostante la grafica simile. A questo punto l'utente è spinto con l'inganno (ad esempio per una "verifica dati") a digitare i propri codici. **Niente di più sbagliato: vengono presto "catturati", con spiacevoli conseguenze**.

Come tutelarsi dalle email truffa? Bastano semplici ma efficaci precauzioni:

A. **Non inserire mai i tuoi dati personali all'interno di email:** La banca non richiede ma i tuoi dati tramite email, né lo farà mai. Nessuna comunicazione "seria" di alcun tipo potrebbe farlo.

B. Imparare a riconoscere le email false: Di solito contengono l'indirizzo del mittente in formato web (es.: nome.cognome@dominio), non sono personalizzate e dichiarano intenti non ben specificati (es.: scadenza dei codici, smarrimento, problemi tecnici o di sicurezza). Spesso usano anche toni "intimidatori", come le minacce di sospensione del servizio in caso di mancata risposta.

C. Non cliccare sui link e non aprire file allegati: I siti web proposti da email sospette non vanno visitati, neppure per brevi periodi. La stessa precauzione vale per i file allegati: mai scaricarli. Se proprio si vuole visitare il link dell'email, ricopiare l'indirizzo completo nell'apposito spazio sul browser, evitando così di ritrovarsi in siti con indirizzi finti. Alle email di spamming non si deve rispondere né cliccare sul collegamento per richiedere la cancellazione dalla lista dei destinatari.

D. Segnalare l'accaduto: Nel caso in cui si riceva un'email sospetta, segnalare l'accaduto al numero verde 800/201510. In alternativa, è opportuno denunciare l'accaduto all'Autorità Giudiziaria o di Polizia.

2) CONTROLLARE LA SICUREZZA DEL SITO PRIMA DI FORNIRE DATI RISERVATI

Non inserire in nessun sito web password o numeri di carte di credito/debito, senza aver prima verificato che la trasmissione dati risulti "sicura" e che il sito web sia autentico. Ecco come fare:

- Verificare sempre la presenza del prefisso **"https://"** nell'indirizzo web.
- Accertarsi che sia presente l'icona **"lucchetto chiuso"** nella barra di stato del browser.
- Controllare se sia attivo il **protocollo SSL 128bit** che protegge le trasmissioni dati. Basta selezionare la funzione "Proprietà" di una pagina (menù tasto destro del mouse), oppure fare un doppio clic sul "lucchetto chiuso".

E' importante ricordare, poi, che la modalità per accedere al sistema di Internet Banking non può cambiare da un giorno all'altro senza una comunicazione ufficiale. Inoltre, diffidare assolutamente di richieste di codici fuori dalle pagine ufficiali del sito, magari in pop-up (una finestra aggiuntiva di dimensioni ridotte). Se dovesse capitare, denunciare segnalare subito l'accaduto

3) EVITARE IL "SALVATAGGIO AUTOMATICO" DELLE PASSWORD SUL BROWSER

I codici di identificazione (Codice adesione e PIN) non devono mai essere "salvati" nella memoria del browser o del Personal Computer. Per sicurezza, verifica che non sia attiva la funzione di "completamento automatico" del browser:

Ad esempio da INTERNET EXPLORER:

- cliccare sul menu "Strumenti" ed attivare "Opzioni Internet";

- cliccare quindi sulla voce "Contenuto" e "Completamento automatico";
- se presente, eliminare il "flag" dalla voce "Nome utente e password sui moduli" e cliccare sui pulsanti "Cancella moduli" e "Cancella password".
- Premere OK e chiudere quindi le finestre di opzioni aperte.

Ad esempio da MOZILLA FIREFOX:

- cliccare sul menù "Strumenti" ed attivare "Opzioni";
- cliccare quindi sulla voce "Privacy", "Impostazioni" e, inserire il "flag" in "Password salvate".
- Premere OK per chiudere la finestra di opzioni.

4) PROTEGGERE IL COMPUTER CON ANTIVIRUS E DISPOSITIVI DI FILTRAGGIO

Per navigare internet è indispensabile installare un programma AntiVirus per proteggersi da eventuali "infezioni provenienti da siti, email, CD masterizzati. Ma non basta installarlo, è consigliabile scaricare periodicamente gli aggiornamenti dal sito del produttore. Esistono poi i dispositivi ***Firewall***, che tengono sotto controllo ciò che entra e ciò che esce dal PC, proprio come dei "buttafuori" digitali.

5) NON CONDIVIDERE FILE SU INTERNET

Condividere file su Internet (con i software per scaricare mp3, video, ecc..) significa lasciare una "porta aperta" a rischio di virus. Particolari software denominati spyware, possono avere facile accesso e "catturare" via Internet informazioni personali a tua insaputa. Evitare di condividere file consente di aumentare la sicurezza. Nel caso si intenda comunque utilizzare la “condivisione”, utilizzare sempre antivirus e firewall.

6) AGGIORNARE SPESSO IL SISTEMA OPERATIVO

Le aziende produttrici dei Sistemi Operativi rendono disponibili online, e scaricabili gratuitamente, gli aggiornamenti degli stessi. Si tratta delle cosiddette patch, che incrementano, tra l'altro, la sicurezza dei programmi. Sugli stessi siti è anche possibile verificare se il browser e i programmi di posta siano aggiornati. Scaricare le patch previene l'utilizzo fraudolento delle cosiddette "vulnerabilità" dei programmi.

Le ricordiamo che in caso di necessità potrà richiedere il **BLOCCO** del servizio di INTERNET BANKING (a scopo precauzionale) rivolgendosi alla propria filiale di competenza oppure contattando il numero verde gratuito **800-837455**.

Cordiali saluti

CENTROVENETO BASSANO BANCA
Credito Cooperativo Soc. Coop.