Oggetto: Attenzione alle truffe informatiche.

Gentile Cliente,

in questi giorni, sfruttando le preoccupazioni che il Coronavirus sta generando tra le persone, i criminali del web stanno approfittando di questo momento di vulnerabilità per colpire le proprie vittime con **attività di Phishing** relative all'**emergenza COVID-19**.

E' necessario pertanto prestare la **massima attenzione nell'aprire email ed allegati** che facciano riferimento a tali comunicazioni, **ricordandosi di controllare sempre il mittente** e **non aprire l'allegato se l'email proviene da un mittente non usuale e/o non atteso**.

Ricordati di **verificare con regolarità che il tuo computer, tablet o smartphone, sia costantemente aggiornato,** sia per quanto riguarda l'**antivirus** sia per quanto riguarda il **sistema operativo**.

Ecco le regole principali per difenderti dalle truffe informatiche:

VERIFICA SEMPRE l'IBAN Durante i pagamenti online controlla sempre l'iban del destinatario presente nel messaggio (SMS o Notify) e le informazioni riportate nelle mail di conferma del bonifico, prestando la massima attenzione che sia quello correttamente inserito.

NON COMUNICARE MAI I TUOI DATI Diffida di qualunque richiesta di dati su carte di pagamento, chiavi di accesso all'internet banking, informazioni personali. La tua Banca non chiede mai queste informazioni elettronicamente (via posta elettronica, sms e altro), neanche per motivi tecnici o di sicurezza.

NON CLICCARE I LINK SU EMAIL E SMS Per connetterti al sito della banca, scrivi direttamente l'indirizzo nella barra di navigazione. Non cliccare su link presenti su email e sms, che potrebbero invece condurti su siti contraffatti, molto simili all'originale.

CONTROLLA IL NOME DEL SITO Verifica l'autenticità della connessione con l'internet banking, 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.

CONTROLLA IL CONTO Verifica periodicamente il tuo conto corrente per assicurarti che le transazioni riportate siano quelle realmente effettuate. Attiva gli strumenti di protezione delle transazioni e-commerce con carte di pagamento.

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

USA SOFTWARE DI PROTEZIONE Installa e mantieni aggiornati software di protezione (antivirus e antispyware), ed effettua delle scansioni periodiche del tuo hard disk.

AGGIORNA COMPUTER E TELEFONO Aggiorna costantemente sistema operativo e applicativi del computer o dello smartphone, installando solo gli aggiornamenti ufficiali disponibili sui siti web o Store delle aziende produttrici.

INSTALLA SOLO PROGRAMMI SICURI Durante la navigazione in internet, installa solo programmi di cui puoi verificare la provenienza.

QUANDO IL COMPUTER RALLENTA 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.

EMAIL SOSPETTE Fai affidamento sul tuo buon senso, usa la dovuta cautela e ricorda le regole d'oro: accertati della sua provenienza, sii prudente con gli allegati e, nel caso in cui l'email contenga un link, ricorda che con il semplice passaggio del mouse sul collegamento puoi verificare il vero indirizzo a cui rimanda.

L'impegno e l'attenzione di tutti è fondamentale per prevenire le truffe informatiche. Grazie per la collaborazione.

BANCA