AVVISO DI SICUREZZA

Gentile Cliente,

alcuni utenti dei Servizi Telematici della Banca di Credito Cooperativo “San Barnaba” di Marino stanno ricevendo in questi giorni una e-mail del tipo:

Gentile Cliente,

Nell'ambito delle misure di sicurezza da noi adottate, controlliamo costantemente le attività del sistema. Durante una recente verifica, abbiamo rilevato un problema riguardante il tuo conto.

Abbiamo deciso di limitare l'accesso al tuo conto fino a quando non verrà completata l'implementazione di misure di sicurezza aggiuntive.

Per controllare il tuo conto e le informazioni che BCC Credito Cooperativo ha utilizzato per decretare di limitare l'accesso al conto, visita il seguente sito:

https:// ……..

Se, dopo aver controllato le informazioni sul conto, desideri ulteriori chiarimenti riguardo all'accesso al conto, contatta il modulo Contattaci nell'Aiuto.

Ci scusiamo per gli eventuali disagi.

Cordiali saluti,

BCC Credito Cooperativo

Tale e-mail non è stata ovviamente autorizzata né spedita da uffici e/o da personale dipendente della Banca, perché la Banca di Credito Cooperativo di Marino **NON CHIEDE MAI LE VOSTRE CREDENZIALI** (username e password) specialmente via posta elettronica.

Se ricevete una e-mail e/o qualsiasi altro messaggio che chiede di inserire le vostre credenziali, anche se il mittente sembra essere affidabile o un vostro conoscente, non apriteli né tantomeno cliccate sui link in essi contenuti e **NON RISPONDETE** ma cancellateli immediatamente, in quanto si tratta certamente di un tentativo di furto di identità (phishing) che ha come obbiettivo di ottenere le vostre credenziali di accesso per poterle poi utilizzare per scopi illegali

Di seguito troverete alcuni utili suggerimenti su come prevenire tali fenomeni di **phishing**, che Vi invitiamo a leggere e seguire con attenzione:

1) **Conservare con cura i Codici Identificativi**
I codici identificativi e, in particolare, **le password di accesso e dispositiva sono strettamente personali e non devono essere comunicate a nessuno**.
Si raccomanda di non attivare la funzione di memorizzazione automatica delle password sul PC, specialmente se questo può essere utilizzato anche da altre persone.

2) **Verificare sempre l'indirizzo del sito**

Per accedere ai vari Servizi Telematici della Banca è sempre opportuno digitare l'indirizzo preciso del sito interessato (nel caso del servizio di Internet Banking della Banca sarà: www.nextbanking.it) ed evitare di utilizzare link presenti su eventuali e-mail, anche se apparentemente inviate dalla Banca stessa, o su altri siti Internet.

3) **Verificare sempre la presenza e i dati del certificato digitale**

Ad ogni accesso, prima di digitare i propri codici identificativi sulla pagina di logon al servizio, verificare sempre la protezione della pagina. A tal fine occorre fare doppio click sul simbolo di "lucchetto" posto nella parte in basso a destra del video e verificare, nella finestra che si aprirà, che il certificato di protezione sia correttamente rilasciato nel caso del servizio di Internet Banking della Banca sarà: "www.nextbanking.it" rilasciato da: "Thawte Premium Server CA").

4) **Mantenere aggiornato il software del proprio PC**

Mantenere sempre aggiornato il sistema operativo del proprio PC e, soprattutto, il software antivirus. Evitare inoltre di installare software o aprire files di cui non si conosce la provenienza.

5) **Utilizzare in maniera appropriata la posta elettronica**

Esaminare le e-mail ricevute evitando di aprire quelle sospette. Considerare sempre assolutamente sospette eventuali e-mail che propongono link con il sito della Banca o con altri siti dove viene richiesto di digitare i propri codici segreti.

Da parte della Banca **non Vi sarà mai richiesto di comunicare le password di accesso e/o qualsiasi altra vostra credenziale di accesso**. Richieste in tal senso, pervenute tramite e-mail o con altro mezzo, devono sempre essere considerate **non attendibili**.