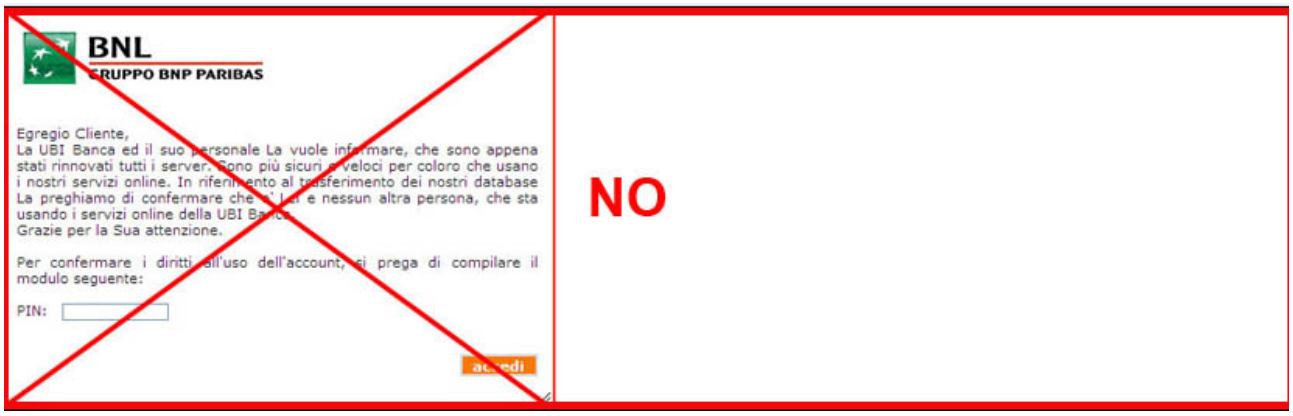
Opera in sicurezza e comodità su e-banking BNL Business

BNL pone la massima attenzione per garantire la sicurezza del tuo conto corrente e per tale finalità utilizza le procedure e le tecnologie più avanzate. Tuttavia, per minimizzare le possibilità di utilizzi fraudolenti associati al tuo conto corrente, è necessario che tu stesso segua alcune semplici regole.

Quali sono le modalità di truffa più frequenti sul web?
Negli ultimi tempi si è diffuso un fenomeno noto con il termine di "Phishing" finalizzato ad acquisire i dati personali e l'identità digitale degli utenti. Il furto di identità viene realizzato solitamente attraverso l'invio di e-mail contraffatte, con la grafica ed i loghi ufficiali di aziende ed istituzioni, che invitano il destinatario a fornire informazioni personali.

Un'altra tecnica recente verso la quale è necessario prestare particolare attenzione è la diffusione di alcuni particolari virus informatici che connettono direttamente ad una pagina "pirata" e non ufficiale di BNL. In questa pagina potrebbe esserti richiesto di aggiornare i dati personali e confermarli con l'utilizzo delle credenziali (PIN e/o OTP).

Di seguito un esempio di una possibile pagina pirata e non ufficiale di BNL a confronto con quella ufficiale :



Come posso difendermi dal Phishing?

- In primo luogo, quando desideri operare con la Banca Via Internet, digita sempre nuovamente l'indirizzo https://business.bnl.it/bway/access/login nello spazio predisposto del tuo navigatore ("browser") e da lì accedi all'Area Riservata.
- Non salvare ("bookmark") l'indirizzo dell'Area riservata all'interno del menù "Preferiti" del tuo browser: potrebbe essere intercettato da virus presenti sul tuo computer.
- Verifica sempre dopo aver inserito le credenziali di accesso, Utente, Password e Numero Postazione, che l'indirizzo nella barra di navigazione del browser sia un sottodominio di business.bnl.it ossia: https://business.bnl.it/bway/portal/
- E' importante aggiornare i programmi usati per navigare in rete: alcune tecniche di phishing utilizzano difetti presenti in vecchie versioni di navigatori ("browser") Internet.
- Installa ed aggiorna costantemente un programma antivirus evoluto.
- Diffida di qualunque e-mail che ti richieda l'inserimento di dati riservati riguardanti: codici di pagamento, codici di accesso o altre informazioni personali e riservate. BNL non richiede mai queste informazioni via e-mail.
- Non cliccare su link presenti in e-mail sospette: questi collegamenti potrebbero condurti a un sito contraffatto, difficilmente distinguibile dall'originale. Di solito il sito presenta loghi e immagini del tutto simili a quelli presenti sul sito originale di BNL, ma spesso sono presenti errori grammaticali che ti aiutano a individuare la provenienza fraudolenta della pagina.
- Diffida di e-mail con indirizzi web molto lunghi, contenenti caratteri inusuali che presentino ad esempio il simbolo "@".
- Quando inserisci dati riservati in una pagina web, assicurati che si tratti di una pagina protetta: queste pagine sono riconoscibili in quanto l'indirizzo che compare nella barra del browser comincia con "https://" e non con "http://" e nella pagina è sempre presente l'icona con il lucchetto, che identifica un sito certificato.

Consigliamo a tutti coloro che hanno fornito dati personali e coordinate bancarie, di monitorare i propri conti per verificare eventuali movimenti non effettuati o non richiesti.
In tale caso, è opportuno procedere con una denuncia presso le forze dell'ordine insieme al blocco del proprio conto corrente e contattare le assistenze dedicate di BNL oppure utilizzando la casella reclami@bnlmail.com.

Per la clientela Professionisti e Imprese è a disposizione il Customer Service (CRC) che risponde al numero verde 800.902.901; per le Aziende e la Pubblica Amministrazione invece, il Servizio Assistenza Corporate (SAC) risponde al numero ripartito 848.78.22.88 (dall'estero:+39 06 9774.4132).