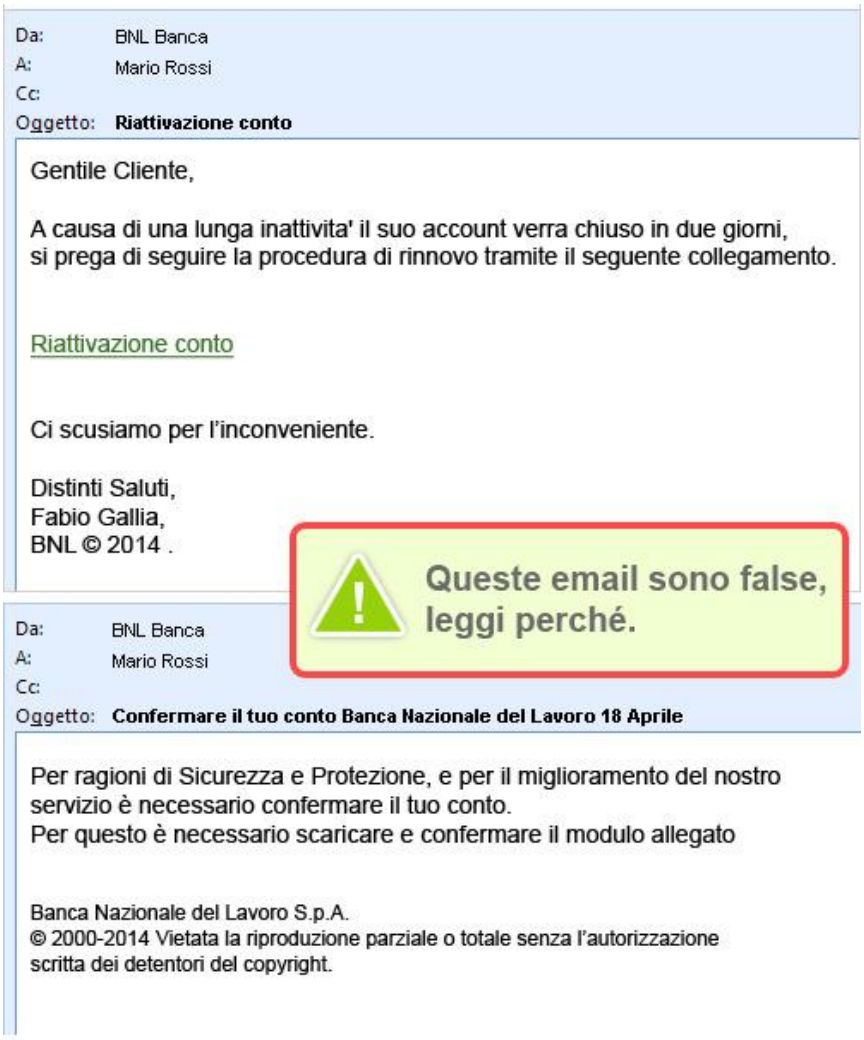
Navigare in sicurezza



Recentemente sono state inviate **email apparentemente di BNL** (negli esempi riportati compare come mittente "BNL Banca"), che invitano a fornire le credenziali di accesso all'area clienti di bnl.it e i dati delle carte di credito.

Si tratta di frodi, ecco perché:

BNL non invia mai email chiedendo di inserire le tue credenziali di accesso o fornendo moduli da compilare con dati delle tue carte di credito!

Ricordati che il Numero Cliente e il PIN, le tue credenziali di accesso all'area clienti di bnl,it, non scadono mai!

Quando nelle email invitano a cliccare su un link falso, l'indirizzo della pagina di atterraggio:

- è privo di lucchetto
- inizia con "http" anziché con "https"
- porta a indirizzi falsi come "namuzaji.com"

Ecco **due semplicissime regole** per difenderti da questo tipo di truffe:

1 non dare mai credito a mail di questo tipo
2 ogni volta che vuoi accedere alla Banca via Internet di BNL, digita manualmente la url "www.bnl.it" nella barra degli indirizzi del tuo browser, e quindi clicca sul pulsante di accesso all'Area Clienti.

In generale, per minimizzare le possibilità di subire una truffa online, ricorda sempre che:

- **BNL non richiede mai l'inserimento contemporaneo di tutti i codici di sicurezza** (Numero Cliente, PIN segreto e OTP)
- L'**OTP** (One Time Password, il codice numerico a 6 cifre generato dal Pass BNL) viene richiesta unicamente in fase di **accesso ai servizi dispositivi** e al momento della **firma di una disposizione**
- **BNL non chiede mai la variazione o la conferma di dati personali o bancari** (codice fiscale, indirizzo, recapito telefonico, dati relativi alle carte di credito etc.): per modificare i tuoi dati personali devi essere tu ad accedere all'Area Clienti di bnl.it e utilizzare il servizio Variazione dati anagrafici.

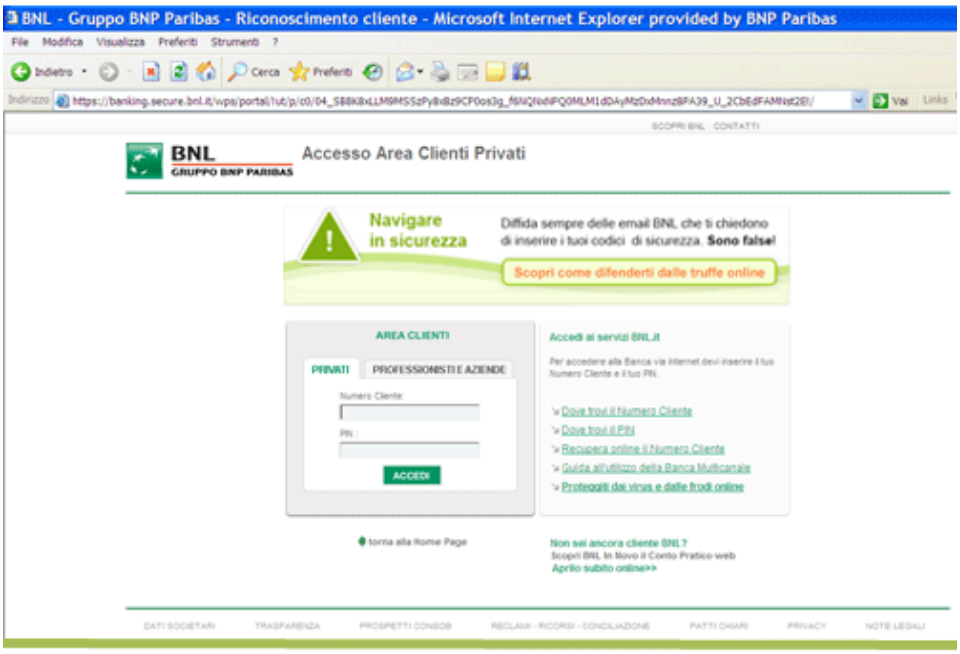
Ecco in pochi passi cosa puoi fare per affrontare il phishing, la frode online oggi più comune:

- osserva bene la struttura della pagina di accesso all'Area Clienti di bnl.it
- confrontala con alcuni esempi di false pagine di accesso create dai cybercriminali
- analizza un esempio di email che imita la grafica di BNL e invita a comunicare informazioni personali e riservate
- leggi tutti i consigli su come difendersi dal phishing
- scopri come aumentare la sicurezza delle tue operazioni.

Falsa pagina di indisponibilità del servizio

Se richiamando la pagina di accesso all'Area Clienti di bnl.it ti trovi di fronte una pagina web come questa, il tuo computer potrebbe essere stato vittima di un virus informatico: **contattaci immediatamente all'800. 900.900** per verificare la situazione ed eventualmente procedere con il blocco degli strumenti di sicurezza e delle tue carte.

La pagina di accesso all'Area Clienti di BNL



DETTAGLIO PAGINA DI ACCESSO AREA CLIENTI

Navigare in sicurezza

Diffida sempre delle email BNL che ti chiedono di inserire i tuoi codici di sicurezza. **Sono false!**

Scopri come difenderti dalle truffe online

AREA CLIENTI

PRIVATI | PROFESSIONISTI E AZIENDE

Numero Cliente:

PIN :

ACCEDI

Accedi ai servizi BNL.it

Per accedere alla Banca via Internet devi inserire il tuo Numero Cliente e il tuo PIN.

- Dove trovi il Numero Cliente
- Dove trovi il PIN
- Recupera online il Numero Cliente
- Guida all'utilizzo della Banca Multicanale
- Proteggiti dai virus e dalle frodi online

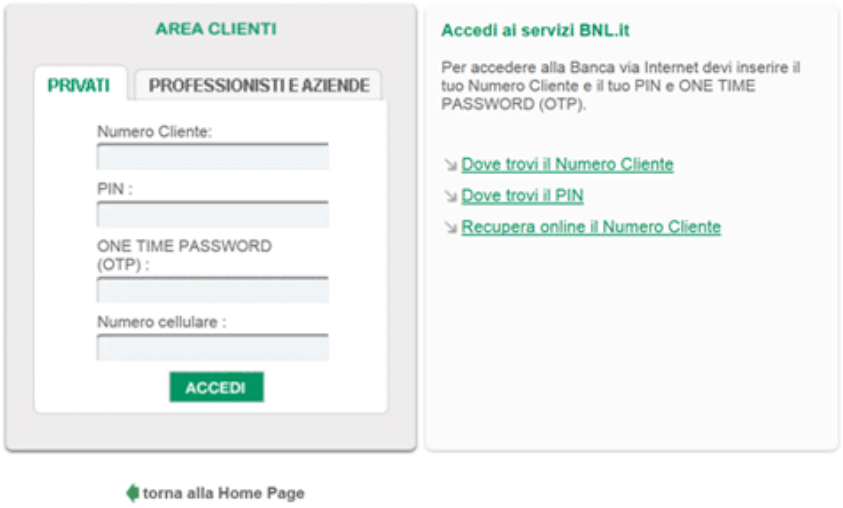
torna alla Home Page

Non sei ancora cliente BNL?
Scopri BNL In Novo il Conto Pratico web
Aprilo subito online>>

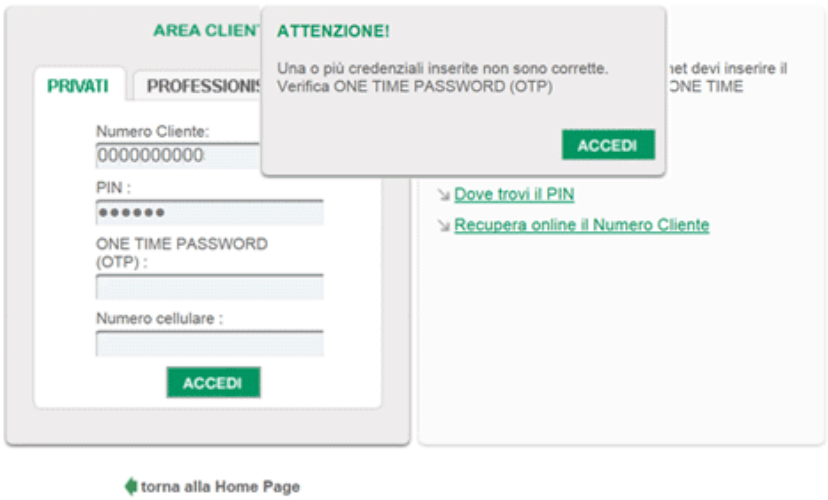
Questa è la pagina ufficiale di BNL: come vedi i codici di sicurezza che richiediamo per l'accesso all'Area Privata sono due e non tre o più.
Ti ricordiamo infatti che l'OTP (One Time Password, il codice numerico a 6 cifre generato dal Pass BNL) viene richiesta unicamente in fase di accesso ai servizi dispositivi e al momento della firma di una disposizione.

Falsa pagina di accesso all'Area Clienti: esempio n. 1

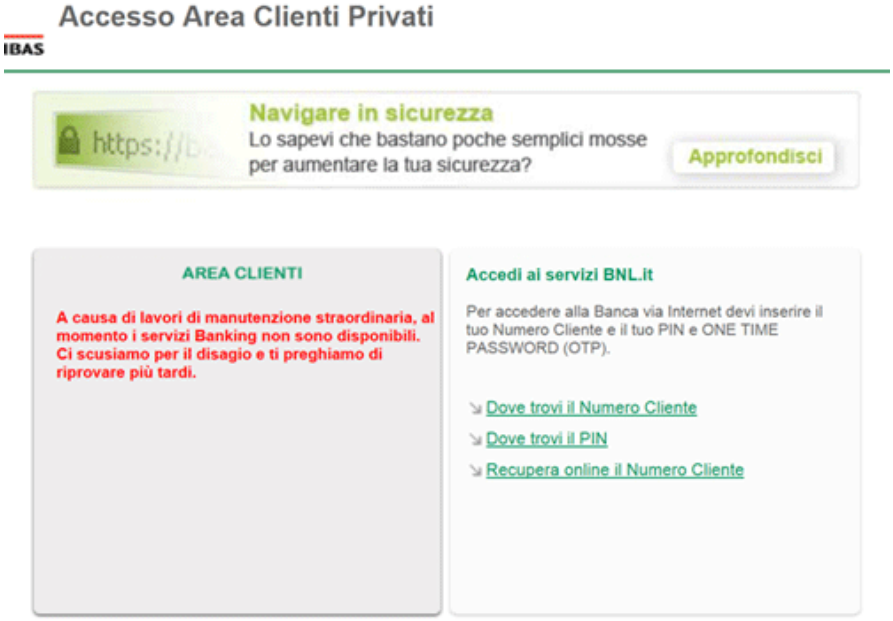
1) Maschera di login con richiesta simultanea di Numero Cliente, PIN, OTP, recapito cellulare



2) Finto messaggio di errore finalizzato a richiedere una seconda OTP



3) Finto messaggio di indisponibilità del sistema

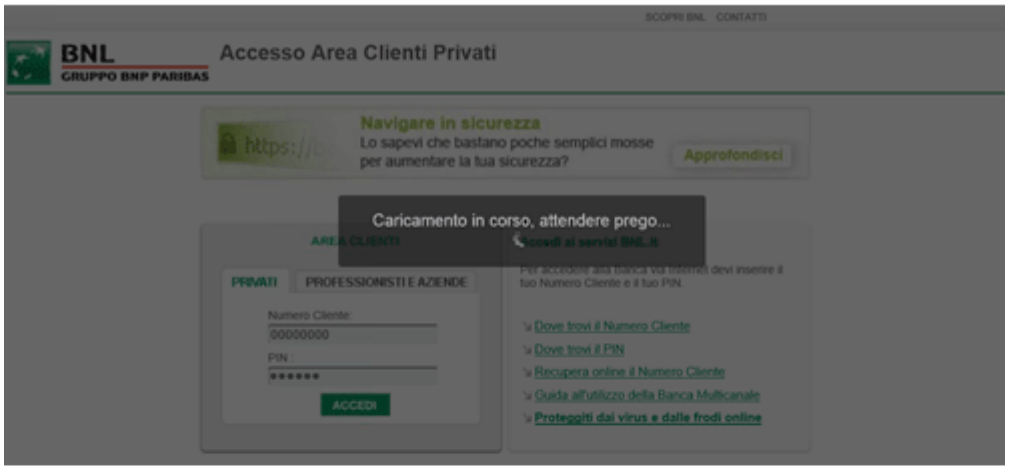


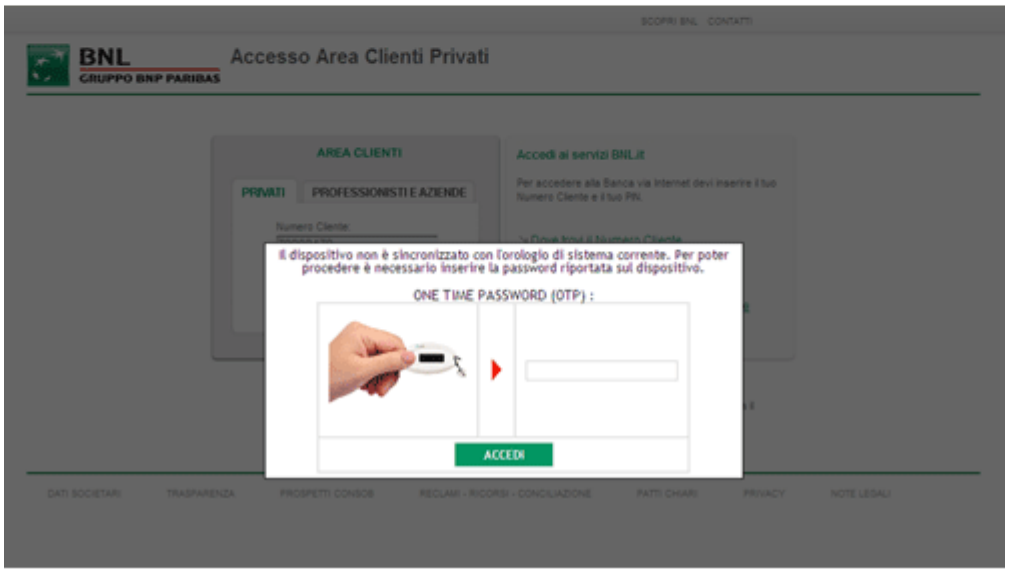
In questo esempio di pagina “pirata” ti viene richiesto di accedere all'Area Clienti del sito inserendo, oltre a Numero Cliente e PIN, anche OTP e numero di cellulare. Il messaggio di errore visualizzato nella schermata successiva invita a inserire nuovamente l'OTP. Infine viene mostrato un messaggio di indisponibilità del sistema.

Attenzione! BNL non chiede mai l’inserimento contemporaneo di tutti i codici di sicurezza (Numero Cliente, PIN segreto e OTP); l'OTP (One Time Password, il codice numerico a 6 cifre generato dal Pass BNL) viene richiesta unicamente in fase di accesso ai servizi dispositivi e al momento della firma di una disposizione.

Se ti trovi di fronte una pagina web come questa non inserire alcun codice e contattaci immediatamente all’800. 900.900 per il blocco degli strumenti di sicurezza e delle tue carte.

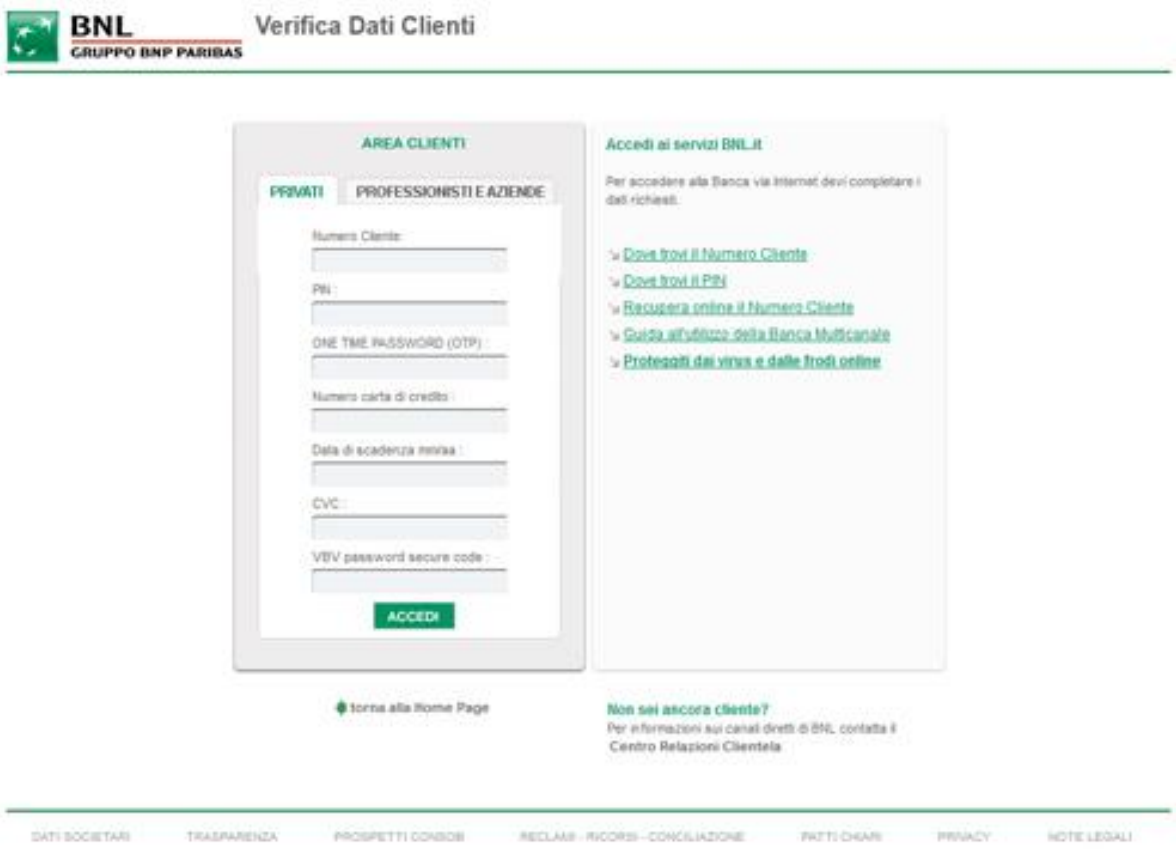
Falsa pagina di accesso all'Area Clienti: esempio n. 2





Le pagine a cui si accede tramite i link contenuti nelle email inviate dai cybercriminali sono molto simili alla nostra pagina ufficiale di accesso all'Area Clienti.
In questo esempio di pagina "pirata" ti viene richiesto di inserire l'OTP all'interno di un popup visualizzato dopo l'inserimento di Numero Cliente e PIN.
Attenzione! BNL non chiede mai l'inserimento contemporaneo di tutti i codici di sicurezza (Numero Cliente, PIN segreto e OTP); l'OTP (One Time Password, il codice numerico a 6 cifre generato dal Pass BNL) viene richiesta unicamente in fase di accesso ai servizi dispositivi e al momento della firma di una disposizione.
Se ti trovi di fronte una pagina web come questa non inserire alcun codice e **contattaci immediatamente all'800. 900.900** per il blocco degli strumenti di sicurezza e delle tue carte.

Falsa pagina di accesso all'Area Clienti: esempio n. 3



Le pagine a cui si accede tramite i link contenuti nelle email inviate dai cybercriminali sono molto simili alla nostra pagina ufficiale di accesso all'Area Clienti.

In questo esempio di pagina "pirata" ti viene richiesto di inserire tutte le tue credenziali di accesso all'area riservata (Numero Cliente, PIN, OTP), nonché i dati relativi alla tua carta di credito.

Attenzione! BNL non chiede mai l'inserimento contemporaneo di tutti i codici di sicurezza (Numero Cliente, PIN segreto e OTP), **né richiede mai la variazione o la conferma di dati personali o bancari** (codice fiscale, indirizzo, recapito telefonico, dati relativi alla carta di credito etc.). Per modificare online i tuoi dati personali devi essere tu ad accedere all'Area Clienti di bnl.it e utilizzare il servizio Variazione dati anagrafici e solo da lì potrai farlo.

Se ti trovi di fronte una pagina web come questa **non inserire alcun codice e contattaci immediatamente all'800. 900.900** per il blocco degli strumenti di sicurezza e delle tue carte.

Falsa pagina di accesso all'Area Clienti: esempio n. 4

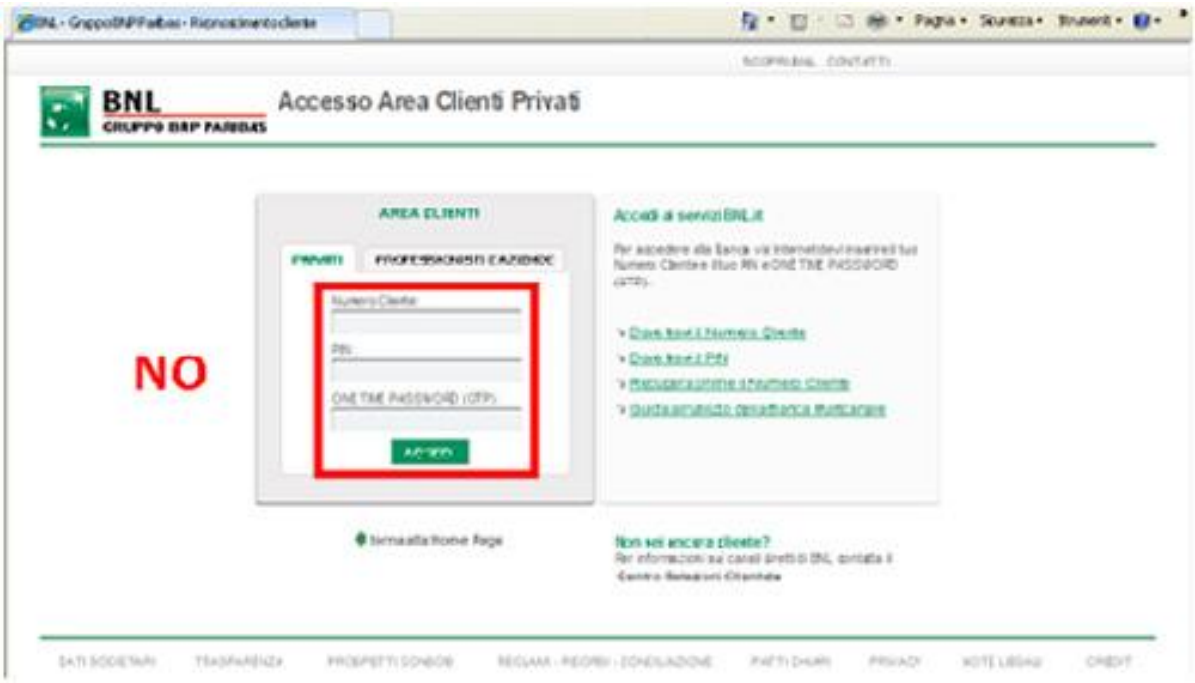
Le pagine a cui si accede tramite i link contenuti nelle email inviate dai cybercriminali sono molto simili alla nostra pagina ufficiale di accesso all'Area Clienti.

In questo esempio di pagina "pirata", per quanto simile a quella del sito BNL, viene richiesto di inserire tutte le tue credenziali di accesso all'area riservata (Numero Cliente, PIN, OTP).

Attenzione! BNL non chiede mai l'inserimento contemporaneo di tutti i codici di sicurezza (Numero Cliente, PIN segreto e OTP); l'OTP (One Time Password, il codice numerico a 6 cifre generato dal Pass BNL) viene richiesta unicamente in fase di accesso ai servizi dispositivi e al momento della firma di una disposizione.

Se ti trovi di fronte una pagina web come questa non inserire alcun codice e **contattaci immediatamente all'800. 900.900** per il blocco degli strumenti di sicurezza e delle tue carte.

Falsa pagina di accesso all'Area Clienti: esempio n. 5



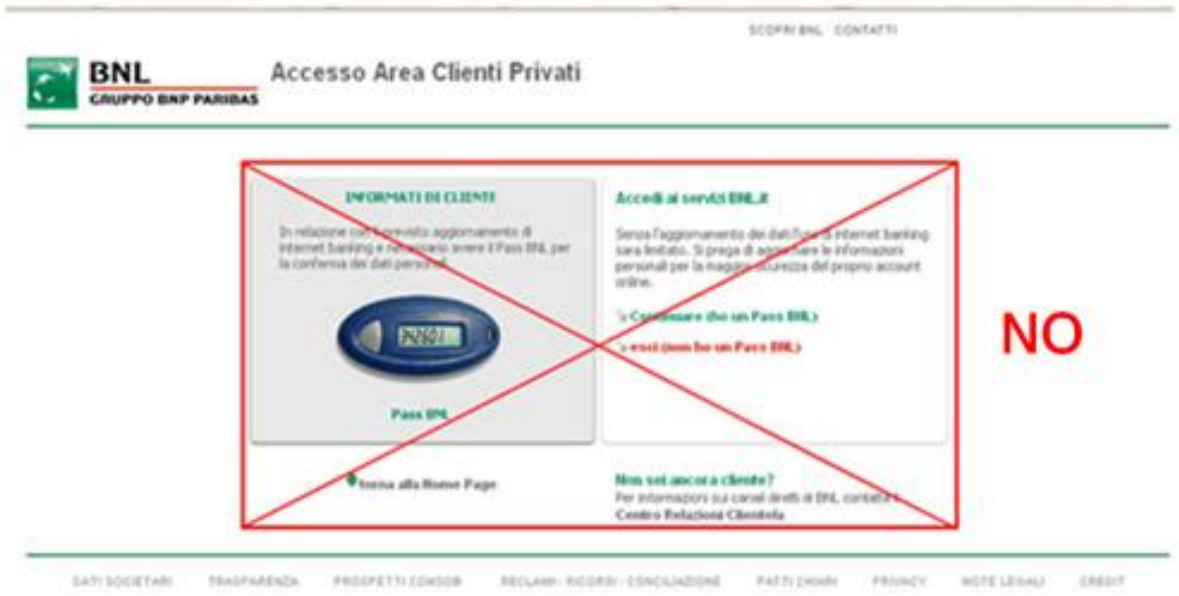
Le pagine a cui si accede tramite i link contenuti nelle email inviate dai cybercriminali sono molto simili alla nostra pagina ufficiale di accesso all'Area Clienti.

In questo esempio di pagina "pirata", per quanto simile a quella del sito BNL, viene richiesto di inserire tutte le tue credenziali di accesso all'area riservata (Numero Cliente, PIN, OTP).

Attenzione! BNL non chiede mai l'inserimento contemporaneo di tutti i codici di sicurezza (Numero Cliente, PIN segreto e OTP); l'OTP (One Time Password, il codice numerico a 6 cifre generato dal Pass BNL) viene richiesta unicamente in fase di accesso ai servizi dispositivi e al momento della firma di una disposizione.

Se ti trovi di fronte una pagina web come questa non inserire alcun codice e **contattaci immediatamente all'800. 900.900** per il blocco degli strumenti di sicurezza e delle tue carte.

Falsa pagina di accesso all'Area Clienti: esempio n. 6



Le pagine a cui si accede tramite i link contenuti nelle email inviate dai cybercriminali sono molto simili alla nostra pagina ufficiale di accesso all'Area Clienti.

In queste pagine "pirata", simili a quelle del sito BNL, potrebbe esserti richiesto di inserire o confermare tutte le tue credenziali di accesso all'area riservata (Numero Cliente, PIN, OTP).

Attenzione! BNL non chiede mai l'inserimento contemporaneo di tutti i codici di sicurezza (Numero Cliente, PIN segreto e OTP), **né richiede mai la variazione o la conferma di dati personali o bancari** (codice fiscale, indirizzo, recapito telefonico, dati relativi alla carta di credito etc.). Per modificare online i tuoi dati personali devi essere tu ad accedere all'Area Clienti di bnl.it e utilizzare il servizio Variazione dati anagrafici e solo da lì potrai farlo.

Se ti trovi di fronte una pagina web come questa non inserire alcun codice e **contattaci immediatamente all'800. 900.900** per il blocco degli strumenti di sicurezza e delle tue carte.

Esempio di email che imita la grafica di BNL

Da: Banca Nazionale del Lavoro S.p.A. [mailto:BNL_sicurezza@bnlmail.com]
Inviato: giovedì 6 settembre 2012 12:59
A: «cognome nome»
Oggetto: Hai un nuovo messaggio di sicurezza

BNL
Gruppo BNP PARIBAS

Gentile Cliente BNL,

Recentemente abbiamo ricevuto degli accrediti non autorizzati sulla carta di credito associata a questo account.

Per motivi di sicurezza il tuo conto online è stato sospeso.

clicca sul link sottostante e verifica i dati richiesti.

http://www.bnl.it/index.html

Solo dopo aver accertato l'autenticità del titolare ripristineremo l'account.

Grazie per la collaborazione,

il reparto di Informazioni e sicurezza.

Banca Nazionale del Lavoro S.p.A.

Sede legale e Direzione Generale
Via V Veneto 119 - Roma

Telefono: 06 47021
Fax: 06 470 20466
E-mail: redazionebnl@bnlmail.com

In passato ha circolato una mail proveniente dall'indirizzo BNL_Sicurezza@bnlmail.com (indirizzo inesistente e non BNL) in cui si avvisa che il proprio account BNL è stato sospeso e che per riattivarlo occorre inserire i propri dati in una pagina web, raggiungibile tramite un apposito link: all'apparenza può sembrare un indirizzo della Banca (es. http://www.bnl.it/index.html) ma in realtà nasconde un sito che nulla ha a che fare con BNL anche se la pagina è molto simile alla nostra pagina ufficiale di accesso all'Area Clienti.

Attenzione! BNL non chiede mai dati di alcun genere tramite mail.

Nel caso in cui tu riceva una mail come questa, **non inserire alcun codice e contattaci immediatamente all'800. 900.900** per il blocco degli strumenti di sicurezza e delle tue carte.

Come puoi notare il mittente è "Banca Nazionale del Lavoro S.p.A. e, anche se non più in uso, è stato utilizzato uno dei vecchi loghi della Banca. La firma inoltre è completa di sede legale e recapiti. E' quindi molto facile cadere nel tranello.
Il testo contenuto nella mail è il seguente:

> *"**Gentile Cliente BNL,***
>
> *Recentemente abbiamo ricevuto degli accrediti non autorizzati sulla carta di credito associata a questo account.*
> *Per motivi di sicurezza il tuo conto online è stato sospeso.*

clicca sul link sottostante e verifica i dati richiesti.
http://www.bnl.it/index.html
Solo dopo aver accertato l'autenticità del titolare ripristineremo l'account.

Grazie per la collaborazione,
Il reparto di informazioni e sicurezza.
Banca Nazionale del Lavoro S.p.A.
Sede legale e Direzione Generale:
Via V.Veneto,119 – Roma

Telefono: 06 47021
Fax: 06 470 20466
E-mail: redazionebnl@bnlmail.com ”

Il phishing (furto di identità): cos'è e come difendersi

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 email contraffatte, con la grafica ed i loghi ufficiali di aziende ed istituzioni, che invitano il destinatario a fornire informazioni personali.
Ecco alcune semplici regole per difenderti dal phishing.

- In primo luogo, quando desideri operare con la Banca Via Internet, digita sempre nuovamente l’indirizzo www.bnl.it nello spazio predisposto del tuo navigatore (“browser”) e da lì accedi alla sezione dedicata cliccando sull'apposito link.
- Non salvare l’indirizzo dell’Area riservata all’interno del menù “Preferiti” (“bookmark”) del tuo browser: potrebbe essere intercettato da virus presenti sul tuo computer.
- Verifica sempre, dopo aver inserito il tuo Numero Cliente e PIN, che l’indirizzo nella barra di navigazione del tuo browser sia un sottodominio di BNL.it:
    - per il banking: https://banking.secure.bnl.it
    - per il trading: https://trading.secure.bnl.it
- Non memorizzare mai nel browser le tue credenziali di accesso a bnl.it (Numero Cliente e PIN)
- 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 email 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 email.

- Non cliccare su link presenti in email 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 email 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 caso di accrediti di questo tipo, è opportuno procedere con una denuncia presso le forze dell'ordine insieme al blocco del proprio conto corrente e contattare BNL ai seguenti recapiti:

800 900 900
reclami@bnlmail.com

Altri consigli per aumentare la sicurezza delle operazioni ed evitare truffe

Esistono alcuni semplici accorgimenti che devi adottare anche tu per evitare che truffatori acquisiscano i dati riservati relativi al tuo conto corrente (intestatario, IBAN, PIN e codici di accesso ai servizi di Banca via Internet e Banca via Telefono) e ne facciano un uso illecito.

- Attiva il servizio **SMS Alert** per ricevere notifiche su: pagamenti e prelievi effettuati con le carte di pagamento, saldo del conto corrente, movimenti sui conti correnti, accesso alla Banca via Internet e Mobile BNL con le tue credenziali. Sottoscrivendo il servizio SMS Alert, inoltre, riceverai gratuitamente le notifiche SMS su tutti i bonifici effettuati da internet e mobile.
- **Verifica i periodicamente i movimenti del tuo conto corrente** nell’Area riservata del sito BNL e i dettagli di quanto riportato sull’estratto conto per controllare che non vengano addebitati pagamenti con assegni o altre transazioni (puntuali o periodiche) da te non effettuati o richiesti. Se individui trasferimenti di denaro che non riconosci di aver effettuato, segnala alla banca la spesa non riconosciuta.
- Non lasciare incustoditi i **libretti degli assegni**.
- **Non comunicare via email le informazioni associate al tuo corrente**.

- Non comunicare mai a nessuno le informazioni associate al tuo conto, anche se queste ti vengono richieste da persone che dicono di contattarti per conto di BNL.
- Ignora le eventuali email che ricevi al tuo indirizzo di posta elettronica e che ti richiedono di connetterti ad un determinato sito (in alcuni casi del tutto simile a quello ufficiale della tua banca) per poi inserire i tuoi dati personali e quelli relativi al tuo conto corrente. **Non rispondere mai a questo tipo di email e non inserire i dati che ti vengono richiesti**.
- Ricordati sempre, quando vuoi buttare documentazione cartacea proveniente dalla banca e contenente dati relativi al tuo conto corrente, di tagliarla in pezzi non ricomponibili.