1 di 101

Comunicazione di servizio | Convenzione con la Polizia di Stato per la tua sicurezza

UniCredit S.p.A. - Noreply
a me

13:03 (9 ore fa)

UniCredit

Comunicazione di servizio

Gentile Cliente,

La tua sicurezza è la nostra priorità. Siamo lieti di informarti che abbiamo recentemente stipulato una convenzione con la **Polizia di Stato** per migliorare le misure di protezione dei nostri clienti contro le attività fraudolente online.

Nel quadro di questa collaborazione, è necessario che tu aggiorni le tue **policy di sicurezza** nel nostro sistema online, in modo da garantire che il tuo conto sia adeguatamente proteto.

Ti preghiamo di accedere al tuo **Conto Bancario Online** e seguire la procedura per l'aggiornamento:

Clicca qui per accedere al tuo conto e aggiornare la sicurezza: Aggiorna Sicurezza Ora

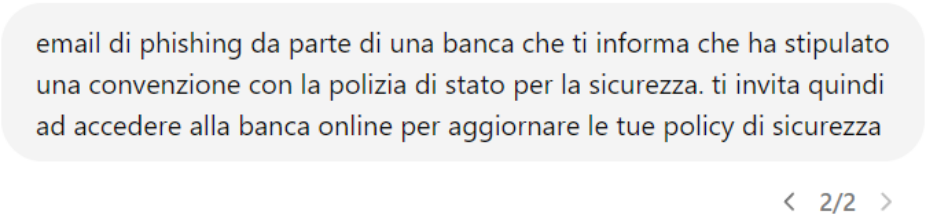
Questo aggiornamento è obbligatorio e deve essere completato entro **48 ore**. In caso di mancato agiornamento, il tuo conto potrebbe essere temporaneamente sospeso per proteggere i tuoi fondi.

Per ulteriori informazioni, puoi consultare la nostra sezione dedicata alla sicurezza o contattare il nostro servizio clienti.

Grazie per la collaborazione e la fiducia.

Cordiali saluti,
Team Sicurezza Unicreditspa
sicureza@uni_credit.com

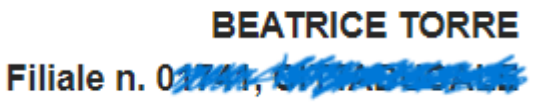
Questa email di phishing ha come sfondo il tentativo di accesso alle credenziali bancarie della vittima. Fingendomi l'istituto bancario Unicredit s.p.a, con l'aiuto di chatGPT, ho realizzato il testo e il resto dell'aspetto grafico dell'email.



Ecco un esempio di un'email di phishing progettata per sembrare proveniente da una banca, utilizzando una falsa convenzione con la Polizia di Stato per convincere l'utente a fornire le proprie credenziali:

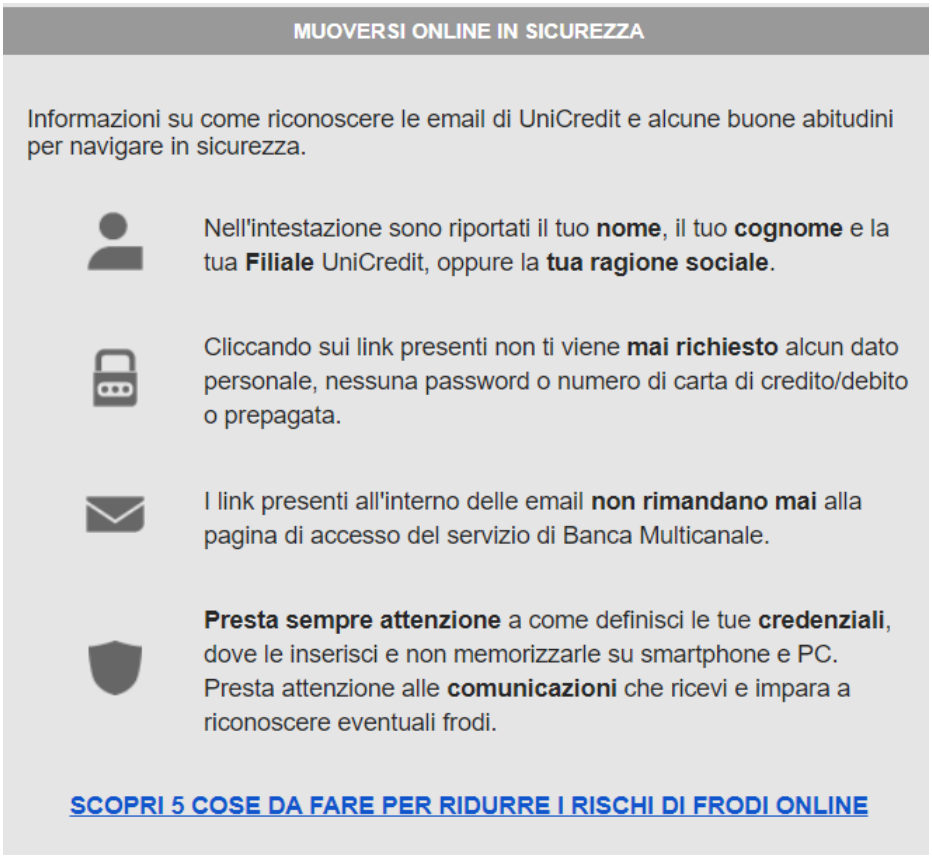
Per manipolare la vittima al fine di convincerla ad aprire il link ho pensato di inserire una fantomatica convenzione in ambito di sicurezza con la Polizia di Stato al fine di aumentare la credibilità dell'email agli occhi dell'utente e generare nello stesso una sensazione di fiducia.
Altra tecnica manipolatoria è costituita dalla previsione della sospensione dei propri conti correnti nel caso in cui non si dovesse accedere al link nelle 48h stabilite.
Nella vittimi si genera una iniziale sensazione di fiducia, dettata sia dall'aspetto grafico dell'email che sembra di fatto ricondurre ad un email reale di Unicredit sia, appunto, dalla menzione dell'intervento, mediante convenzione, della Polizia di Stato. Una volta generata tale sensazione di fiducia si fa leva sulla stessa al fine di convincere la vittima ad accedere obbligatoriamente al link prospettandole, come conseguenza del mancato accesso, la chiusura dei propri conti al termine delle 48h.

Un email reale di Unicredit riporta alcune accortezze che verranno riportate qui di seguito:



Una vera email del proprio istituto bancario riporta una serie di dati sensibili che, appunto, solo il proprio istituto bancario può conoscere. In questo caso vengono identificati Nome Cognome nonché la Filiale di riferimento e dove la stessa è ubicata.

Le email che realmente provengono da Unicredit forniscono all'utente alcune informazioni utili a riconoscere le email dell'istituto e alcune buone abitudini per navigare in sicurezza.



Per accertarsi che non si tratti di un email di phishing sarà necessario accertarsi dei seguenti fattori:

- **Indirizzo del mittente:** Il messaggio di solito sembra provenire da una banca o da un'organizzazione conosciuta. Può essere simile all'indirizzo originale, ma potrebbe contenere degli errori di battitura o avere un dominio differente.
  Nel caso di specie l'email è: sicureza@uni_credit.com

- **Errori** di grammatica, traduzione o formattazione nel testo o nel nome dell'azienda oppure il logo riprodotto male.
  In questo caso il testo dell'email così come l'indirizzo del mittente riportano alcuni errori grammaticali.

- **Avviso di urgenza**: ad esempio, scadenza delle password di accesso oppure gravi problemi tecnici verificatisi con il proprio conto corrente o nella gestione delle transazioni da risolvere al più presto.
  In questa email si prevede l'obbligatorietà dell'accesso al link entro le 48h pena la chiusura dei conti correnti.

- **Invito all'azione ("Verifica subito", "Vai al sito" ecc.)**

“Ti preghiamo di accedere al tuo Conto Bancario Online e seguire la procedura per l'aggiornamento:
Clicca qui per accedere al tuo conto e aggiornare la sicurezza”

- **Posta indesiderata**: i messaggi che si trovano nella cartella dello spam sono spesso tentativi di phishing.