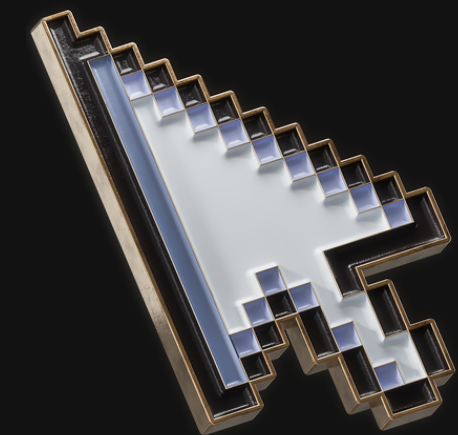


S5-E5



Phishing



Simulazione email di phishing

Scenario


Mail proveniente dalla banca recante notifica di accesso non autorizzato sul conto.

Accesso non autorizzato al suo conto bancario



bank_recovery@libero.it

A: Utente corrente

← Rispondi ← Rispondi a tutti → Inoltra  ...

ven 01/11/2024 03:18

Gentile Cliente,

Abbiamo rilevato un accesso sospetto al suo conto bancario il giorno 31 ottobre 2024 alle ore 21:34. Per motivi di sicurezza, le chiediamo di verificare le sue informazioni e confermare la sua identità.

Per completare la verifica, segua questo link sicuro:

[Conferma la tua identità](#)

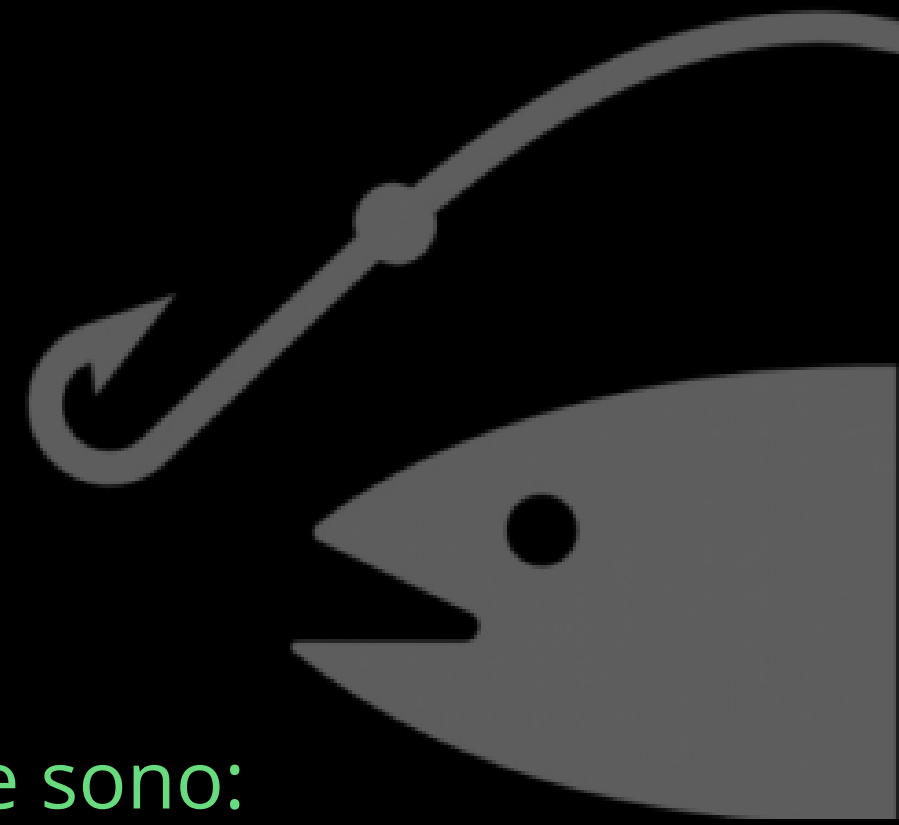
La mancata verifica entro le prossime 24 ore comporterà la sospensione temporanea del suo conto per proteggerlo da accessi non autorizzati.

Non condivida mai i suoi dati personali con nessuno e utilizzi questo link solo per completare la verifica.

Per qualsiasi ulteriore informazione, può contattare il nostro servizio clienti al numero verde **800 123 456**.

Grazie per la collaborazione,
Servizio Assistenza Clienti
Gruppo BCC ICCREA

Finalità



L'obiettivo è sin da subito mandare in agitazione il bersaglio, le parole chiave sono:

“Accesso non autorizzato” e “Mancata verifica = Sospensione”.

L'idea è creare una sensazione di necessaria tempestività per accertarsi che il conto non sia intatto ed evitare problemi maggiori nei giorni successivi a causa di una sospensione del conto. La mail ha la finalità di sottrarre le credenziali di accesso al conto bancario, all'interno del corpo della mail è presente un link, scritto in modo tale da nascondere il vero e proprio URL che, in caso non fosse celato, finendo sotto gli occhi del bersaglio potrebbe essere preso in esame. Il link porterà a una pagina di autenticazione fraudolenta, una volta inserite le credenziali, queste saranno immediatamente ricevute dal mittente della mail di phishing.

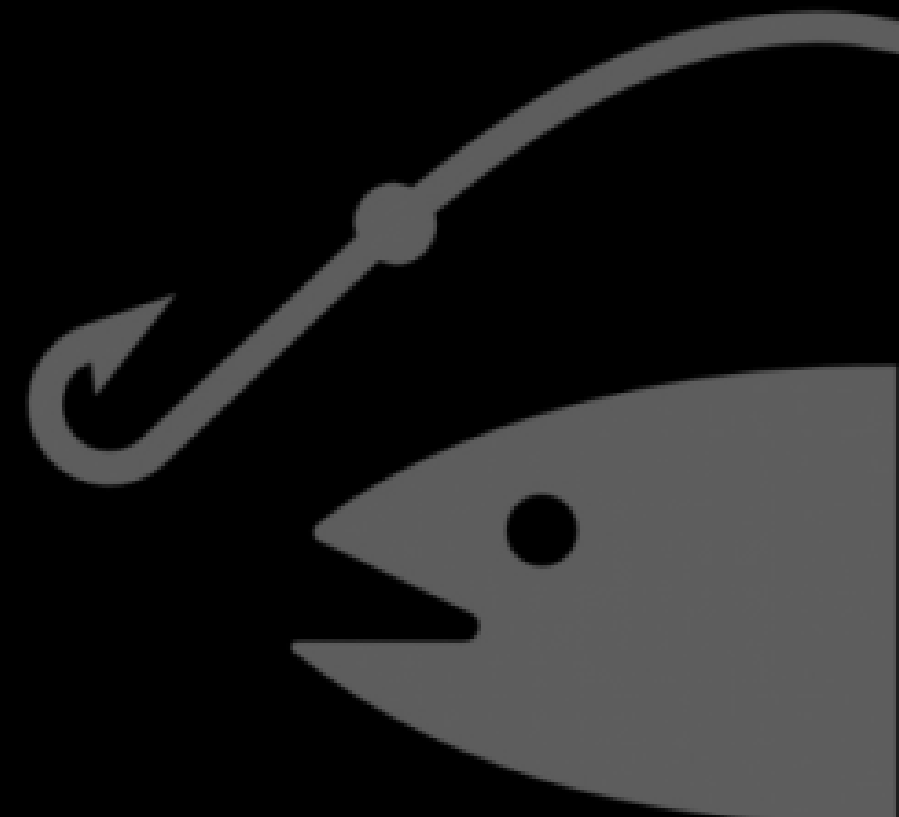
Osservazioni

Soffermandoci con più attenzione ai particolari, possiamo notare elementi d'allarme:

Primo fra tutti l'indirizzo email del mittente, in questo caso, privo di dominio appartenente alla banca sottoindicata nella mail. Assolutamente associabile a una mail qualunque.

Secondo elemento d'allarme è la modalità di verifica identità, una banca non chiederebbe mai una convalida mediante mail.

Terzo, la cartella in cui troviamo la mail, se non fosse nella "posta in arrivo" bensì nella cartella "Spam" o "Posta indesiderata" bisognerebbe già vedere con sospetto la mail poichè evidentemente non ha superato i sistemi di autenticazione: SPM, DKIM e DMARC.



bank_recovery@libero.it

A: Utente corrente

Gentile Cliente,

Abbiamo rilevato un accesso sospetto e ti chiediamo di confermare la tua identità.

Per completare la verifica, segui questo link:

[Conferma la tua identità](#)