

Creare una simulazione di un'email di phishing utilizzando ChatGPT.

OBIETTIVO: Ottenere le credenziali di accesso dell'utente ad un sito web

Si è chiesto a ChatGPT di creare una email di avviso di Poste Italiane. Di seguito il risultato:

Oggetto: Attività Importante sul suo account Poste Italiane

Gentile cliente,

La informiamo di un'attività recente sul suo account di Poste Italiane che potrebbe richiedere la Sua attenzione. Ecco i dettagli dell'azione:

Tipo di Attività: Tentativo di accesso

Data e Ora: 16:12 UTC+1

Indirizzo IP: 10.112.50.174

Posizione Approssimativa: Milano, Italia

Se hai effettuato questa azione, nessuna ulteriore azione è necessaria da parte Sua.

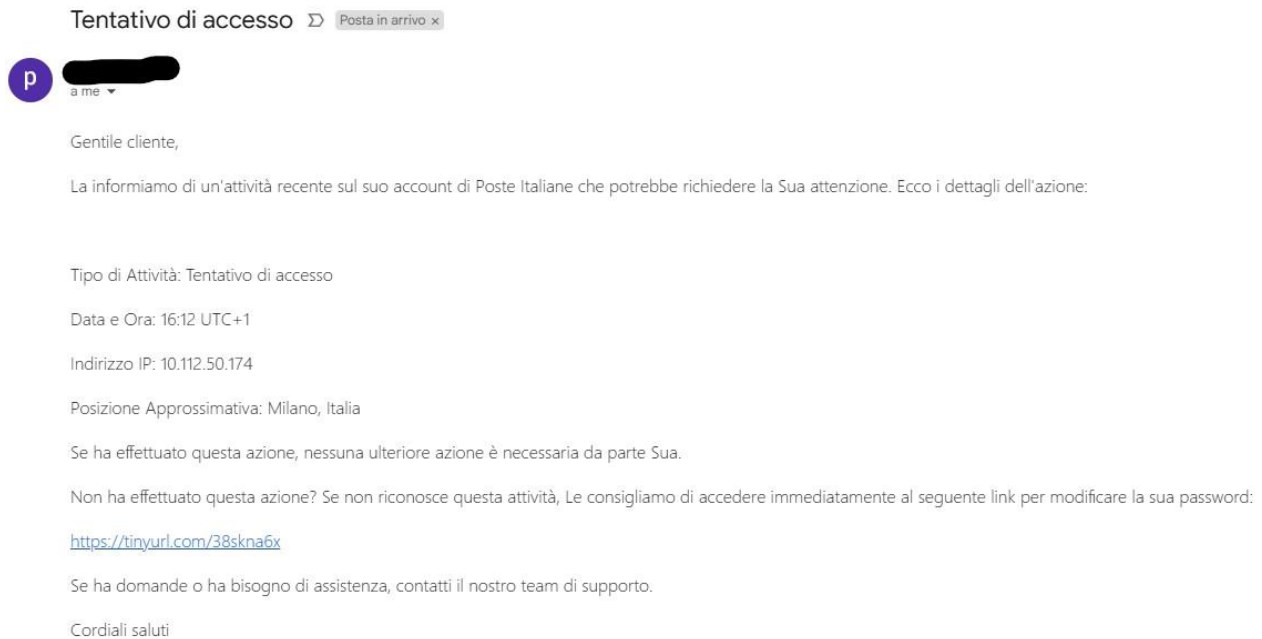
Non ha effettuato questa azione? Se non riconosce questa attività, Le consigliamo di accedere immediatamente al seguente link per modificare la sua password:

<https://tinyurl.com/38skna6x>

Se ha domande o ha bisogno di assistenza, contatti il nostro team di supporto.

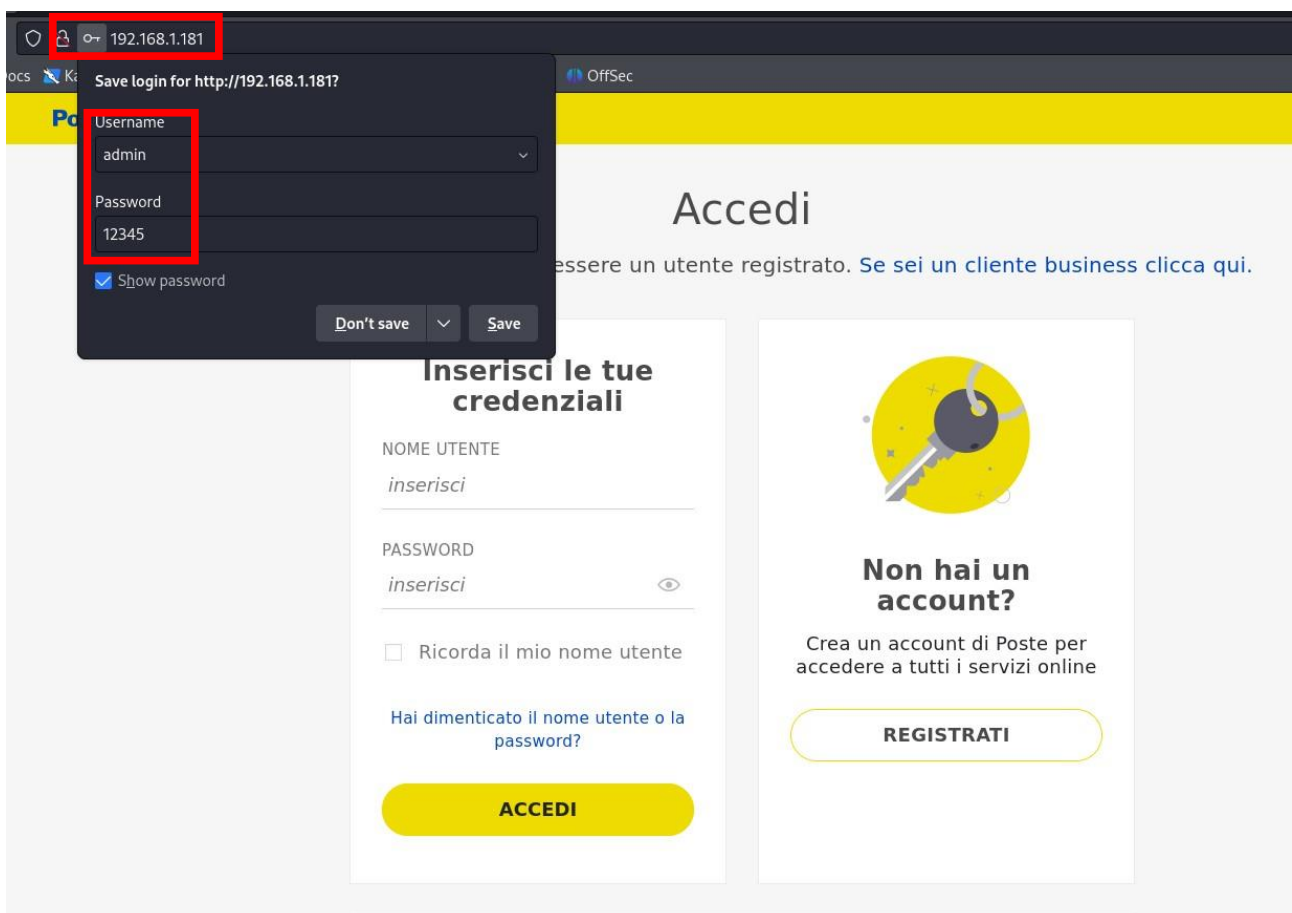
Cordiali saluti

Questo testo è stato poi inviato da una mia email ad un'altra mia email.



Nella mail è stato inserito un link creato con tinyurl per mascherare l'ip privato della macchina Kali. Tramite il toolkit SET, è stato possibile copiare la pagina di login del sito di Poste Italiane che ha lo scopo di intercettare le credenziali di accesso della vittima, hostata sull'indirizzo ip di Kali (192.168.1.181).

Nell'immagine seguente la pagina clonata:



Nell' immagine si possono notare anche le credenziali di test utilizzate:

Username: admin

Password: 12345

Una volta utilizzate le credenziali di test sulla pagina clone di login di Poste Italiane, esse compaiono anche nel toolkit SET.

```

remement_module_activitymap", "blackberrylocationcollector", "browserdetection", "domdatacollection", "domaindetection", "fingerprint", "html5locationcollector", "hashtable", "ie_fingerprint", "interactionelement", "mozilla_fingerprint", "opera_fingerprint", "rsauievent", "timer", "uielementlist", "visitor", "_dom_data_collection2", "accordionopenbyurl", "activeonscroll", "activexdetect", "addeventlistener", "add_deviceprint", "aiutaci_a_migliorare", "aiutaci_a_migliorare_biz", "alert", "anchorscrollingtofocus", "animationscrollaccordion", "apripannel", "lomenue", "atob", "blur", "btoa", "buildlink", "callbackdrop", "cancelanimationframe"], "excludeld": [{"size": 0, "count": 0}], "truncated": true}, "inputs": [{"no_name", "checkbox-remember", "dep", "dep", "dop", "dop", "evp", "evp", "mid", "password", "rememberme", "securetoken", "signature", "username"}, {"iframes": [], "scripts": [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 593, 0, 1065, 0, 0, 0, 0, 949, 307, 240, 0, 0, 0, 0, 1603, 0, 0, 0, 189, 6, 63, 606, 1791, 3136, 3812, 2986], "collection_status": 0}
PARAM: evp=1,1, INPUT:text,5@1,3,0;1,4,0@0,1583,0,1
PARAM: mid=
PARAM: rememberme=
POSSIBLE USERNAME FIELD FOUND: username=admin
POSSIBLE PASSWORD FIELD FOUND: password=123456
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

```

In questo modo possiamo ottenere le credenziali della potenziale vittima ed effettuare il login sul sito attendibile del servizio.

CONSIDERAZIONI

Il contesto della mail creata, fa riferimento ad una situazione di attacco tramite Phising. Il Phising è un tipo di attacco che avviene principalmente tramite email, che sembra provenire da fonti affidabili, attuato per ottenere informazioni riservate dalla vittima, attraverso richieste, uso di link o allegati.

In questo caso la mail descrive un tentativo di accesso non autorizzato nell' account dell'utente. Questo tipo di email, sono legittime, se inviate da fonti attendibili, come un'azienda che fornisce un servizio o prodotto. Servono a tutelare e proteggere il cliente da accessi fraudolenti.

Data la criticità della situazione che descrivono, queste email, sono utilizzate dagli attaccanti per creare uno stato di angoscia, urgenza o minaccia. Questo serve a far agire in fretta l'utente, che spinto da queste sensazioni, non ha tempo di ragionare in maniera lucida sul da farsi e reagire in modo appropriato.

Questo tipo di email, di solito, hanno degli elementi che possono indurre a far dubitare della veridicità del loro contenuto e dell'autenticità della fonte da cui provengono. Questi elementi possono essere:

- *Indirizzo email del mittente*, verificare che l'indirizzo email del mittente sia quello ufficiale.
- *Errori di grammatica e ortografia*: molte email di phishing contengono errori di grammatica, sintassi o traduzioni approssimative.
- *Richiesta di dati personali o bancari*: le aziende affidabili, come le banche, non chiederanno mai via email dati sensibili.
- *Link sospetti*: passare il cursore sopra i link (senza cliccare) per vedere l'URL completo. Spesso i link di phishing portano a siti web che somigliano a quelli ufficiali, ma con URL leggermente diversi.
- *Allegati sospetti*: le email di phishing possono contenere allegati come file .exe, .zip o .scr, che possono contenere malware.
- *Offerte troppo allettanti*: promesse di vincite, offerte troppo vantaggiose o rimborsi inattesi sono spesso usati per attirare le vittime.
- *Firma non professionale*: le aziende di solito includono una firma con informazioni dettagliate di contatto e logo. Una firma generica o poco professionale può indicare un'email di phishing.

Oltre a questi elementi, più facili da controllare ad un'occhiata veloce, ce ne sono altri che si possono controllare, andando a fare una ricerca più approfondita per chi è esperto in ambito di cyber security.

Questi parametri sono fattori di autenticazione e sono installati nel server di chi riceve l'email, non di chi invia. Sono tre:

- *SPF*: è un protocollo di autenticazione email progettato per rilevare e bloccare email di spoofing. Esso controlla l'indirizzo IP del mittente.

- *DKIM*: è un protocollo di autenticazione email che controlla l'identità del mittente (attraverso firma digitale) e l'integrità del contenuto dell'email (attraverso l'hashing).
- *DMARC*: è un protocollo di autenticazione email che utilizza SPF e DKIM per determinare se un'email è legittima. Invia fisicamente l'email solo se uno dei due parametri o entrambi, hanno esito positivo.