Progetto S5

Simulazione di un attacco phishing

Allo scopo di comprendere appieno l'obbiettivo di un attacco phishing, si è pensato a uno scenario ipotetico, volto a simulare un contesto realistico in cui un'email di phishing potrebbe essere inviata.

Nello scenario ipotizzato, è stata presa come esempio una qualsiasi persona che usufruisca dei servizi di Poste Italiane, e che dopo essersi iscritta ai servizi online che essa offre, dopo qualche tempo riceve una mail abbastanza allarmante la quale riporterà un possibile tentativo di accesso all'account della nostra vittima. In una società odierna in cui si parla spesso di furto di identità e fuga di informazioni, chiunque sarebbe allarmato da una comunicazione del genere, spingendo i più impulsivi e ignari, e cliccare sul link presente nella mail pur di salvaguardare i propri dati sensibili.

Immagina di ricevere un'email che sembra provenire da Poste Italiane e che ti avverte di un accesso sospetto al tuo account. L'email ti invita a seguire un link per cambiare le tue credenziali, facendo leva sulla tua preoccupazione per la sicurezza del conto. L'obiettivo è senza dubbio farti cliccare su un link fraudolento per rubare le tue informazioni personali, eppure la preoccupazione è cosi alta, che in molti non ci pensano due volte prima di cadere in trappola.

Struttura della email malevola

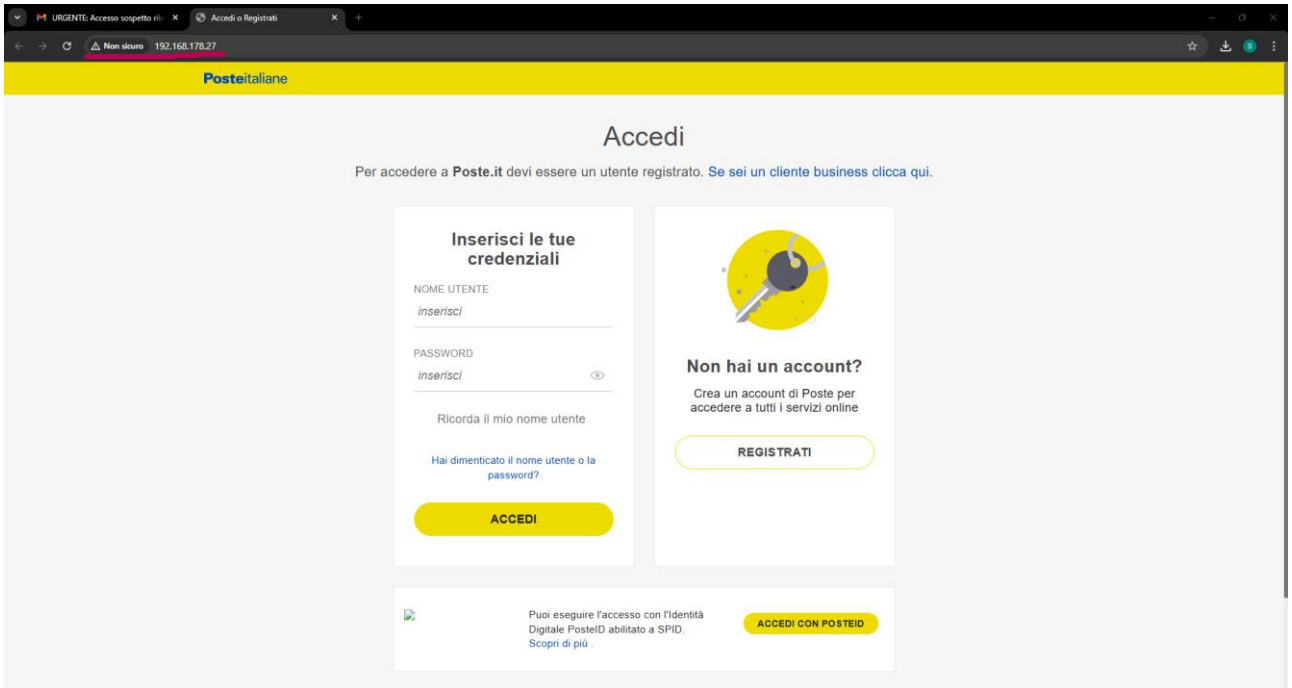
Affinché l'attaccante risulti credibile risulti credibile e allarmante al punto da istigare la vittima a fare il gioco dell'attaccante, al fine di rimembrare una possibile mail inviata da Poste Italiane, essa è stata strutturata in modo molto simile ad una mail con la quale veniva inviata una notifica di autenticazione, dopo l'avvento dello SPID; uno stesso metodo viene utilizzato anche per l'avviso di un eventuale documento scaduto. Questo è un ottimo modo per indurre la vittima a pensare che essa provenga effettivamente dal mittente che lei crede che sia; elementi che vanno dalla struttura del testo fino ad una immagine ben piazzata possono davvero indurre in inganno. Anche se può sembrare credibile vi sono però delle accortezze di cui tener conto.

- **Mittente**: esso potrebbe essere contraffatto, e a volte potrebbe davvero trarre in inganno perché la variazione potrebbe essere un semplice "-" e la vittima quasi sicuramente non noterà la differenza.
- **Allarmismo della mail**: Quando una mail risulta essere molto allarmante, presentando un oggetto come "IMPORTANTE: Aggiornamento delle credenziali richiesto per la sicurezza del tuo account", è proprio perché l'intenzione è quella di creare panico e urgenza inducendo la vittima ad agire il più velocemente possibile.
- **Saluto generico**: le mail di phishing di questo tipo, iniziano molto spesso con saluti generici, cordiali, come Gentile cliente, invece di utilizzare il nome completo della persona. Le banche e Poste Italiane stessa, di fatto, utilizzano proprio il nome della persona a cui sono rivolte le comunicazioni, così come i provider della rete internet.
- **Corpo del messaggio**: potrebbe essere scritto in modo da sembrare formale e autoritario, utilizzando frasi che inducono, proprio come l'oggetto della mail, preoccupazione.
- **Link sospetti**: le mail di questo tipo presentano sempre dei link o immagini (steganografia) che reindirizzino sulle pagine in cui l'attaccante vuole che andiate. I link potrebbero apparire attendibili ma molto spesso sono camuffati, traendo quindi in inganno.
- **Richiesta di dati sensibili**: questo tipo di email chiede di accedere al link malevolo affinché vengano inseriti informazioni sensibili come ID bancario, email, password, PIN, ma molte aziende affidabili, non richiederebbero MAI queste informazioni tramite email.
- **Firma generica e poco professionale**: la firma potrebbe includere un nome generico come "Servizio Clienti Poste Italiane" presente nella mail, ma senza alcun tipo di recapito o contatto ufficiale.

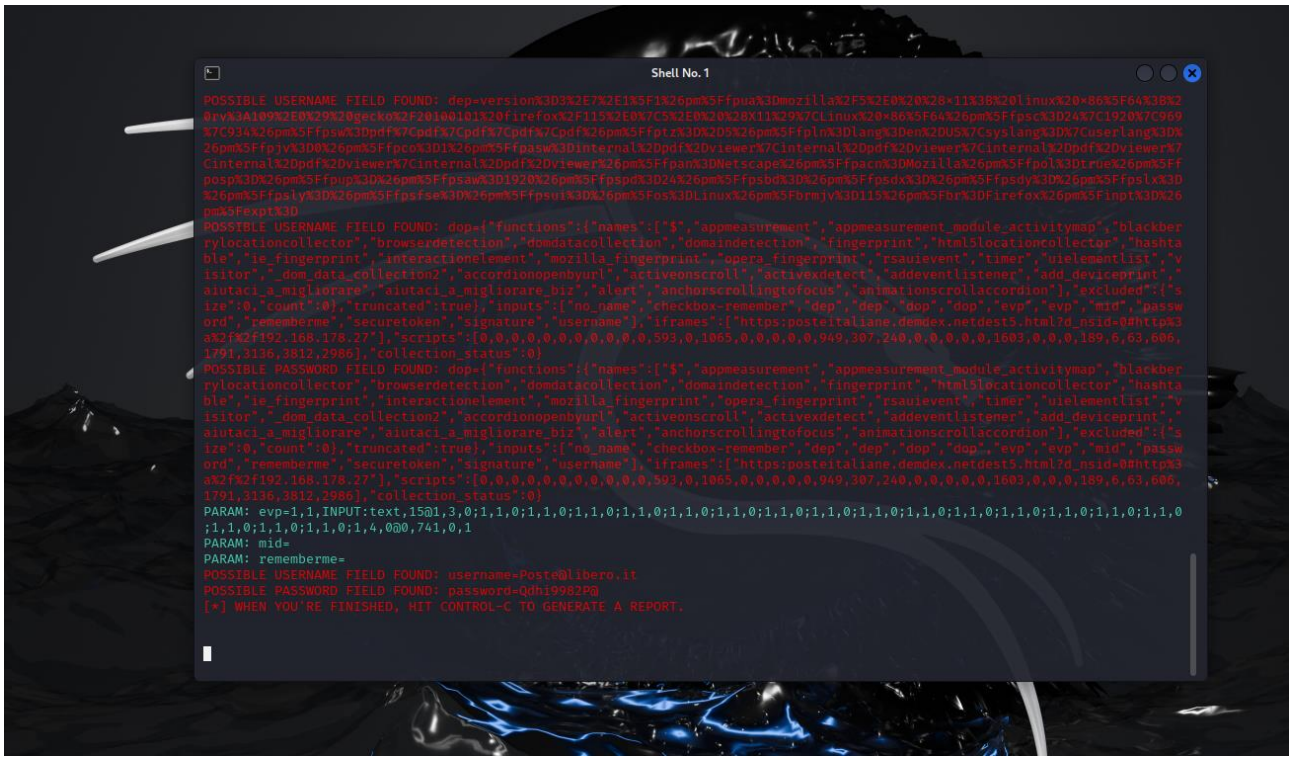
Questi sono alcuni punti molto forti, presenti nella mail che abbiamo scritto, che ci consentono di capire se la mail che andiamo ad analizzare sia malevola o meno. Non sono valori assoluti, né gli unici, ma forniscono una buona panoramica, in modo particolare per chi non è avvezzo al mondo informatico.

Come funziona una email di phishing

Il compito di una email di phishing è quello di portare la vittima all'interno di una pagina infetta, oppure di fronte alla pagina di login del fantomatico mittente verificato. Nel secondo caso, solitamente quando si clicca sul link malevolo si viene reindirizzati su una pagina in cui una volta inserite le credenziali, esse verranno sniffate dall'attaccante senza alcuna difficoltà.



Questo sarà lo scenario in cui si ritroverà chiunque si faccia raggirare dal link malevolo. Ci ritroveremo di fronte ad una pagina di login identica a quella originale, in cui una volta inseriti i dati di accesso:



Saranno resi visibili in chiaro al fautore della mail di phishing.

Cosa si può fare allora per distinguere il reale dal fittizio?

Oltre a dirci che il sito non è sicuro (e quello delle poste lo è) nella barra dell'URL è presente un elemento che in modo innegabile ci garantisce che siamo su una pagina farlocca e pericolosa, ovvero un indirizzo IP privato. Nessun indirizzo IP privato ha infatti la possibilità di navigare in rete. La possibilità che si presenti un IP privato è però non molto comune se ci troviamo a casa, poiché per poter accedervi è necessario essere connessi alla medesima rete locale, motivazione in più per non connettersi alle reti pubbliche di bar o dei parchi ad esempio. A volte però cliccarci sopra potrebbe essere già troppo tardi. Nel test eseguito ciò è stato effettuato a scopo illustrativo, ma se fosse stata una vera mail di phishing i miei dati, o il mio dispositivo a seconda delle intenzioni dell'attaccante, sarebbero andati.

E se ciò avvenisse mentre sono a casa? O in azienda?

Ovviamente in queste circostanze l'attacco di phishing può arrivare da qualunque parte del mondo. È bene quindi informarsi su come difendersi da questa tipologia di attacchi, con alcune accortezze che potrebbero rivelarsi veramente importante.

Come difendersi dal phishing?

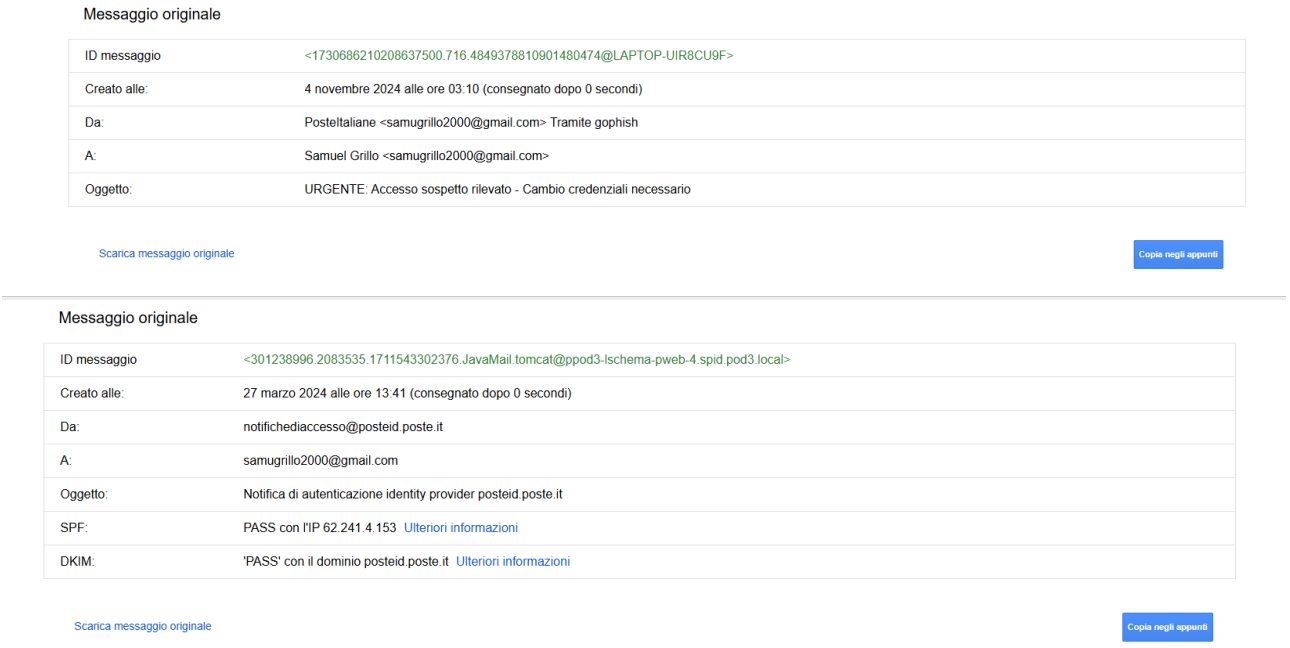
Per difendersi dagli attacchi di phishing sono necessarie alcune accortezze.

- **SPF** – **DKIM** – **DMRC**: sono i 3 moschettieri della sicurezza in ambito phishing. Sono 3 parametri fondamentali per verificare l'identità del mittente e l'integrità della mail stessa. **L'SPF** fa un controllo dell'indirizzo IP del mittente, tramite tabelle e database. Il **DKIM** verifica l'integrità del file, confrontando quindi i codici hash al fine di verificare se la mail si stata compromessa. Il **DMARK** combina invece i due protocolli, fornendo istruzioni chiare su come gestire le email che falliscono

l’autenticazione, indicando se debbano essere scartate messa in quarantena o segnalate come spam.

- **Verificare l’indirizzo del mittente**
- **Controllare tono del messaggio, la grammatica**: riflettere su urgenza e linguaggio utilizzato può davvero aiutare a seconda del mittente. Le istituzioni di questo genere (come banche, poste etc.) non solo utilizzano il nome della persona, ma non si pongono in modo così drammatico. Inoltre è possibile che in queste email fittizie siano presenti degli errori grammaticali che possano quindi indicare che non si tratti di un messaggio attendibile.
- **Ispezionare i link senza cliccarli**: è possibile verificare l’indirizzo effettivo semplicemente passandoci sopra con il cursore; esso comparirà in basso a sinistra della nostra pagina attuale.
- **Controllare firma e dettagli di contatto**: è generica? Mancano contatti o informazioni verificabili? Istituzioni di questo genere sono molto precise, per cui se questi elementi non sono presenti, meglio scartare l’email.
- **Incoerenza della richiesta**: l’aggiornamento delle credenziali non viene mai chiesto tramite email, e viene specificato in molte email provenienti dalle Poste stesse, in qualunque messaggio di risposta automatica. Per ogni dubbio è inoltre possibile consultare il supporto clienti che chiarirà eventuali dubbi.

SPF DKIM DMARC e campanelli di allarme



Messaggio originale

ID messaggio	<1730686210208637500.716.4849378810901480474@LAPTOP-UIR8CU9F>
Creato alle:	4 novembre 2024 alle ore 03:10 (consegnato dopo 0 secondi)
Da:	Posteltaliane <samugrillo2000@gmail.com> Tramite gophish
A:	Samuel Grillo <samugrillo2000@gmail.com>
Oggetto:	URGENTE: Accesso sospetto rilevato - Cambio credenziali necessario

Scarica messaggio originale

Copia negli appunti

Messaggio originale

ID messaggio	<301238996.2083535.1711543302376.JavaMail.tomcat@ppod3-lschema-pweb-4.spid.pod3.local>
Creato alle:	27 marzo 2024 alle ore 13:41 (consegnato dopo 0 secondi)
Da:	notifichediaccesso@posteid.poste.it
A:	samugrillo2000@gmail.com
Oggetto:	Notifica di autenticazione identity provider posteid.poste.it
SPF:	PASS con l'IP 62.241.4.153 Ulteriori informazioni
DKIM:	'PASS' con il dominio posteid.poste.it Ulteriori informazioni

Scarica messaggio originale

Copia negli appunti

Qui sono presenti le differenze tra una email veritiera, affidabile, la quale, provenendo da un mittente verificato avrà superato i controlli di SPF e DKIM in questo caso, e la mail duplicata tramite Gophish, che invece non avrà nessuno dei 3 parametri di sicurezza. Questo è molto importante, soprattutto in aziende, dove bisognerebbe formare il personale, affinché verifichi costantemente tramite sé questi 3 parametri siano presenti all’interno della mail. Se si la mail 9 volte su 10 sarà sicura, anche se vi è una piccola possibilità che questi controlli possano essere elusi. Anche se ciò fosse, è comunque nota bene adoperare in modo efficace questa tipologia di controllo, in modo che anche chi non sia molto informato, possa salvaguardare sé stesso, l’azienda, e le informazioni

Punti deboli nell'email creata

Nell'email inviata a scopo di test, se analizzata, si può notare che sono presenti le caratteristiche sopra citate come errori grammaticali, tono urgente e drammatico, link per cambio credenziali, non viene utilizzato il nome del destinatario, il dominio dell'email non sembra appartenere alle Poste Italiane; tutti elementi che senza dubbio fanno scattare immediatamente un campanello d'allarme. Inoltre se si confronta la mail con altre verificate, si noterà che manca il banner di risposta automatica solitamente presente con questa tipologia di mail, nonché eventuali numeri per il contatto al supporto tecnico.