

Formazione ingegneria sociale

Epicodesecurity



Alessio Golfetto 15/12/2023

Programma Corso

- 9:00 - 10:00 Nozione di ingegneria Sociale
- 10:00 - 10:30 Principali attacchi di ingegneria sociale
- 10:30 - 10:45 Coffee Break
- 10:45 - 12:30 Phishing e come difenderci
- 12:30 - 13:00 Come riconoscere una mail phishing

Ingegneria Sociale

Di cosa parliamo?

L'ingegneria è una forma di manipolazione psicologica che utilizza la debolezza e l'errore umano piuttosto che le vulnerabilità tecniche o digitali del sistema.

I criminali informatici utilizzano spesso questo metodo per appropriarsi di dati personali/aziendali/finanziari che possono poi utilizzare per commettere illeciti.

Alcuni tipi di attacchi di ingegneria sociale

- Phishing (via mail)
- Smishing (via sms)
- Vishing (via voce/chiamate)

Ne esistono altri, ma per oggi ci concentreremo soprattutto sul primo, cioè il phishing che è il metodo più utilizzato per attaccare aziende.

Phishing

Cosa è?

Gli attacchi phishing sfruttano un'e-mail, apparentemente proveniente da una fonte fidata, che richiede informazioni. Un classico sono le mail che sembrano provenire da una banca, che chiede ai propri clienti di "confermare" le informazioni di sicurezza, dirottandoli così su un falso sito dove le credenziali di accesso verranno registrate. Oppure una e-mail che prende di mira una singola persona all'interno di una azienda, inviando una mail che pare provenire da un dirigente di alto livello, che richiede informazioni confidenziali.

Come difenderci

- **Consapevolezza:** l'istruzione delle persone sulla rilevazione delle e-mail di phishing è fondamentale. Le persone devono essere consapevoli dei segnali di un potenziale attacco, come errori di ortografia, indirizzi e-mail sospetti o richieste di informazioni sensibili.
- **Verifica delle Fonti:** le vittime devono verificare attentamente la fonte del messaggio, specialmente quando si tratta di richieste di informazioni sensibili. La verifica può includere contattare direttamente l'azienda o l'organizzazione apparentemente coinvolta.

Come difenderci

- **Uso di Filtri Anti-Phishing**: l'utilizzo di filtri anti-phishing può aiutare a bloccare e-mail sospette prima che raggiungano le caselle di posta degli utenti.
- **Autenticazione Multifattore (MFA)**: l'implementazione di MFA può aggiungere uno strato di sicurezza, anche se le credenziali vengono compromesse.
- **I filtri** : SPF, DKIM, DMARC.

Come riconoscere una mail phishing

- **Controllare sempre il mittente:** quasi sempre nei casi di phishing l'indirizzo e-mail del mittente avrà delle differenze (ortografiche o di dominio della mail). Per esempio potrebbe arrivarvi una mail da "amazon.servizio.clienti@gmail.com" (amazon usa mail con il proprio dominio @amazon, quindi eventuali altri indirizzi sono potenzialmente fake) oppure una mail con mittente "posteritaliane@gmail.com" dove il nome del sito viene leggermente modificato. Nel vostro caso di azienda, dovrete sempre verificare che le mail abbiano come dominio @semoforti.com

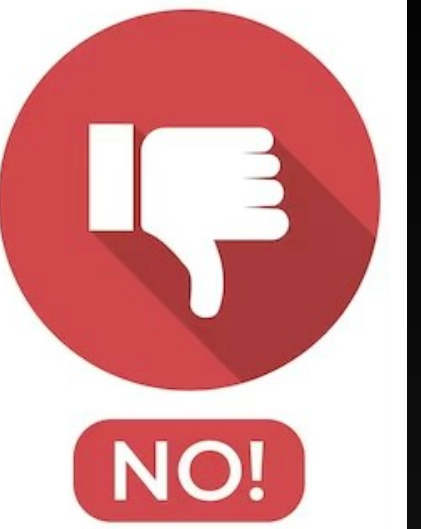
Come riconoscere una mail phishing

- **Ortografia:** solitamente nei messaggi di spam ci sono degli errori ortografici, o di grammatica, anche impercettibili a una prima lettura. Spesso si tratta di traduzioni mal fatte, e che comunque richiedono da parte dell'utente un'azione. Verifica bene il testo prima di fare qualsiasi cosa.

Come riconoscere una mail phishing

- **Header:** non è altro che l'intestazione della mail. Basta dare un rapido sguardo ad altre due voci oltre che al mittente per capire se quella che stiamo aprendo è potenzialmente una mail di phishing. Aprendolo per esteso troveremo le voci "SPF" e "DKIM", accanto ad entrambe le diciture dovremo trovare una voce che ci conferma che il controllo **è stato superato**.

Alcuni esempi di mail reali vs fake



Messaggio originale

ID messaggio	<1702535764885356600.6332.8543051994045262048@Amm01>
Creato alle:	14 dicembre 2023 alle ore 07:36 (consegnato dopo 2 secondi)
Da:	pcroad1408@gmail.com Tramite gophish
A:	Manuel Pinto <pcroad1408@gmail.com>
Oggetto:	Il tuo ordine Amazon.it che include "TP-Link TL-WPA7517 Kit..."

E-mail con mittente
estraneo, dominio differente

[Scarica messaggio originale](#)

[Copia negli appunti](#)

```
Return-Path: <pcroad1408@gmail.com>
Received: from Amm01 ([51.179.99.160])
    by smtp.gmail.com with ESMTPSA id w10-20020a05600c474a00b0040b2c195523sm25514056wmo.31.2023.12.13.22.36.07
    for <pcroad1408@gmail.com>
    (version=TLS1_3 cipher=TLS_AES_128_GCM_SHA256 bits=128/128);
    Wed, 13 Dec 2023 22:36:07 -0800 (PST)
From: pcroad1408@gmail.com
X-Google-Original-From: test@gmail.com
Mime-Version: 1.0
Date: Thu, 14 Dec 2023 07:36:05 +0100
X-Mailer: gophish
Message-Id: <1702535764885356600.6332.8543051994045262048@Amm01>
Subject: Il tuo ordine Amazon.it che include "TP-Link TL-WPA7517 Kit..."
To: Manuel Pinto <pcroad1408@gmail.com>
Content-Type: multipart/alternative; boundary=aa11febf883667e105310ba87ac20e2ee62277d8b0a69861a4262f9eff1d
```


Il tuo ordine Amazon.it che include "TP-Link TL-WPA7517 Kit..." Posta in arrivo x

pcroad1408@gmail.com

a me ▼

Mittente e contenuto non corrispondono

gio 14 dic, 07:36 (1 giorno fa)



[I miei ordini](#)

[Il mio account](#)

[Amazon.it](#)

Ricezione ordine

Ordine n° 405-9927171-5481934

Gentile Manuel,

Grazie per il tuo ordine. Ti invieremo un'e-mail quando i tuoi articoli saranno spediti. La tua data di consegna prevista è indicata in basso. Puoi consultare la sezione [I miei ordini](#) su Amazon.it per visualizzare lo stato del tuo ordine o apportare delle modifiche.

Arriverà:

martedì, dicembre 28

La tua modalità di spedizione è:

prime Premium

La tua preferenza di spedizione:

Spedisci gli articoli non appena disponibili

[Visualizza i dettagli dell'ordine](#)

L'ordine sarà spedito a:

**manuel
acilia, Roma
Italia**

Totale Ordine:


EUR 59,78

Metodo di pagamento
selezionato:

Mastercard

No, grazie



 TP-Link TL-WPA7517 Kit Powerline WiFi, AV1000 Mbps su Powerline, 750 Mbps su WiFi Dual Band, 1 Porta **EUR 59,78**



nale

<0102017dfdbd8244-985293aa-0b28-4ff9-a95e-06a42f49964f-000000@eu-west-1.amazonses.com>		
27 dicembre 2021 alle ore 22:13 (consegnato dopo 0 secondi)		
"Amazon.it" <conferma-spedizione@amazon.it>	←	Mittente conosciuto/congruo con
manuelpinto1408@gmail.com		
Il tuo ordine Amazon.it di "TP-Link TL-WPA7517 Kit..." è stato spedito.		
PASS con l'IP 54.240.1.118 Ulteriori informazioni	←	Controllo SPF passato
'PASS' con il dominio amazon.it Ulteriori informazioni	←	Controllo DKIM passato
'PASS' Ulteriori informazioni		

originale



Amazon.it <conferma-spedizione@amazon.it>

me

Mittente e contenuto corrispondono

lun 27 dic 2021, 22:13

☆ 😊 ↩ ⋮

I miei ordini | Il mio account | Amazon.it

Conferma spedizione

Ordine: #405-9927171-5481934

Ciao,

Abbiamo pensato che potesse interessarti sapere che abbiamo spedito il tuo ordine.

Il tuo ordine è andato a buon fine e non può più essere modificato. Se hai bisogno di restituire un articolo o gestire altri ordini, visita I miei ordini Amazon.it su

In arrivo:

martedì, dicembre 28

Verifica lo stato della spedizione

Il tuo ordine è stato inviato a:

manuel
acilia, Roma

Totale ordine: EUR 59,78

Gli articoli sono stati inviati da Amazon Logistics. Il tuo numero di spedizione è: BA0508070999. A seconda del metodo di spedizione utilizzato, è possibile che le informazioni di tracciabilità possano non essere visibili immediatamente.

Se disponi di un dispositivo mobile, puoi utilizzare gratuitamente [Amazon mobile App](#) per ricevere le notifiche di consegna e monitorare il tuo collo in viaggio.

Visita le nostre pagine di aiuto per [le informazioni di contatto del corriere](#).

Riepilogo ordine

Domande e Feedback



100%

Grazie per la vostra attenzione

Phishing controllato

Prima di tutto chiederei all'azienda il permesso per poter eseguire tale operazione, una volta ottenuto informerei il presidente o chi per esso delle eventuali problematiche aziendali a cui potrebbe andare incontro effettuando questo "test". Lo informerei che alcuni dipendenti vittime di questo phishing potrebbero rimostrare delle lamentele verso l'azienda, magari verso lui stesso e arrivare a querelarlo perché si sentono prese in giro.

Premesso ciò proseguirei con la formazione al personale, dato che saranno loro le "vittime" di questo phishing controllato e per verificare se abbiano appreso o meno come riconoscere un attacco debbono prima esser stati formati.

Finita il corso di formazione farei passare del tempo prima di lanciare il phishing controllato, sfruttando il fatto che il personale se lo aspetta un po' meno rispetto al periodo immediatamente successivo al corso.

Nel mentre tramite il sito getgophish.com, creerei una mail simile a quella aziendale, ad esempio *epicodesecurity@gophish.com*.

Comprerei un dominio di un sito web molto simile all'originale, come ad esempio *www.epicodesecurity.org* oppure *www.epicodesecuity.it* e clonerei la pagina del sito dove i dipendenti devono effettuare il log in per accedere alla loro area riservata.

Come step successivo, per far cadere il maggior numero di persone nella trappola, sceglierei un argomento su cui tutti siano più o meno sensibili, in questo caso la busta paga. Creerei una mail ad hoc per ingannare il dipendente in modo che sia portato ad inserire il suo user e password.

Questa sarebbe la mail che manderei ai dipendenti come test

EpicodeScurity epicodesecurity@gophish.com

a me ▼

Gentile collaboratore,

a causa di un problema tecnico riscontrato nei nostri server, le tue credenziali per accedere al controllo della ricezione e verifica della busta paga sono state erroneamente cancellate.

Ti invitiamo a cliccare sul link sottostante e inserirle nuovamente, l'operazione richiederà meno di un minuto.

Link: www.epicodesecurity.org

Ci scusiamo per il disagio

Grazie della tua preziosa collaborazione

Una volta informato il presidente della data di partenza del test, inizierei a mandare la mail ai vari dipendenti coinvolti. Una volta lanciato l'attacco terrei monitorati report che gophish.com ci restituisce in modo da avere una panoramica chiara su come hanno reagito le persone alla mail phish.

Se il numero di attacchi andati a segno dovesse esser trascurabile suggerirei al presidente di far visionare le slide alle persone che hanno fallito il test. Se invece il numero di attacchi andati a segno fosse elevato e quindi molte persone fossero cascate nel tranello suggerirei lui di effettuare una nuova formazione, in modo da ribadire ancora i concetti.