EPICODESECURITY

Al giorno d’oggi parlare e capire cos’ è l’ingegneria sociale è fondamentale, poiché sempre più persone cascano nei tranelli dei criminali informatici, a mio avviso la colpa e la disinformazione, cercherò di spiegare in breve cos'è l’ingegneria informatica e come proteggersi.

INGEGNERIA SOCIALE:

L’ingegneria sociale è una disciplina che sfrutta processi cognitivi di influenzamento, inganno e manipolazione per indurre una persona a compiere un’azione o a comunicare informazioni riservate. I principali metodi di ingegneria sociale sono Phishing, Infiltrazione Fisica e Social Engineering su Social Media. Questo mondo purtroppo e in costante evoluzione infatti stanno nascendo nuove tecniche di ingegneria sociale come i QR CODE.

PHISHING

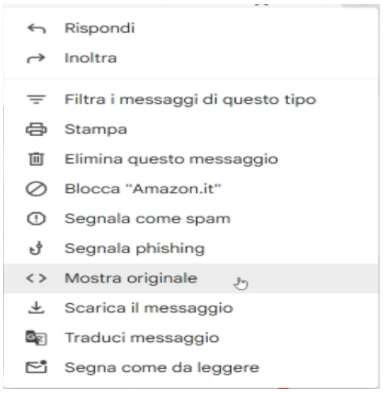
Il phishing è un crimine che inganna le vittime inducendole a condividere informazioni sensibili quali password e numeri di carte di credito.Vi sono modi diversi di indurre la vittima ad abboccare all'amo, ma esiste una tattica di phishing più diffusa: La vittima riceve un'e-mail o un messaggio di testo che imita una persona o organizzazione di cui si fida, ad esempio un collega, un istituto bancario o siti di spedizione (amazon,gls). L'e-mail o il messaggio contiene informazioni volte a spaventare la vittima, con la richiesta di visitare un sito web e intraprendere azioni immediate per evitare conseguenze negative.

Se l'utente "abbocca all'amo" e fa clic sul link riportato nel messaggio, viene indirizzato sull'imitazione di un sito web legittimo. A questo punto, all'utente viene richiesto di accedere inserendo le proprie credenziali: nome utente e password. Se l'utente è abbastanza ingenuo da eseguire la richiesta, le informazioni inserite saranno trasmesse al criminale che potrà utilizzarle per rubare identità, intercettare accessi a conti bancari e vendere informazioni personali sul mercato nero.

COME DIFENDERSI DAL PHISHING

I principali metodi per difendersi dal phishing sono SPF,DKIM,DMARC che ora spiegheremo cosa sono e come fare a vederli, ci tenevo a ricordare che tutti possono cadere in questi tranelli, anche le persone più attente, infatti la prima difesa contro il phishing è la mentalità, non pensare frasi del genere "a me non può succedere" o "sono troppo intelligente per cascarci", poiché è proprio questa sicurezza che i criminali informatici usano contro di noi. Capiamo dove andare a controllare la provenienza di una e-mail e dove controllare SPF,DKIM,DMARC. Bisogna andare sulla mail cliccare i tre puntini in alto a destra come nella foto

Una volta cliccato si aprirà una serie di scelte dove noi dovremo andare a selezionare "Mostra originale" come nella foto

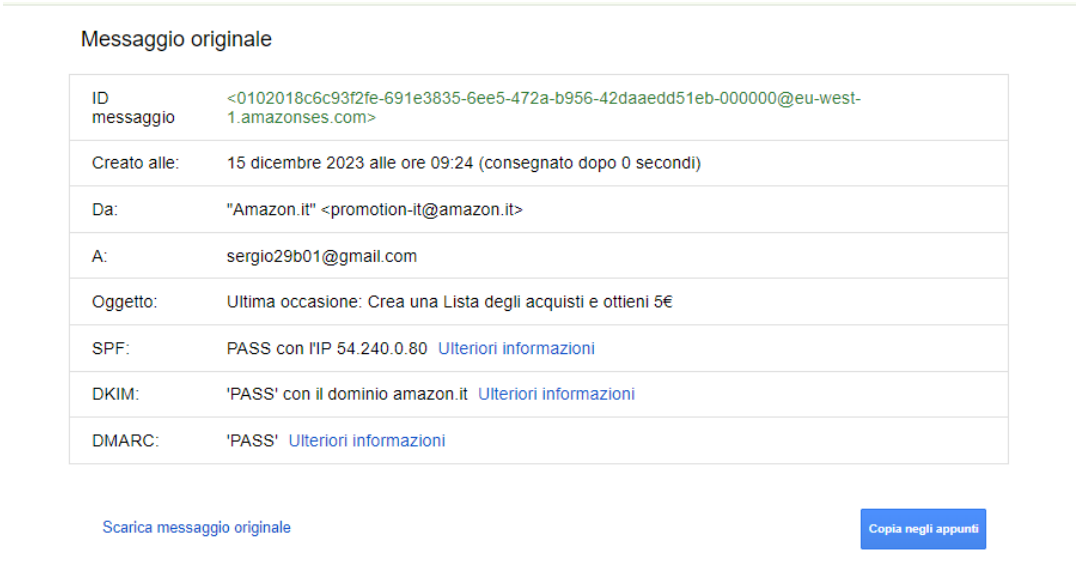


Prima spieghiamo a cosa servono SPF,DKIM,DMARC

SPF (Sender Policy Framework): Serve per verificare che l'indirizzo IP del mittente della mail sia autorizzato a farlo per conto del dominio specificato.
L'autorizzazione si ha perché in precedenza il proprietario del dominio ha specificato nei record DNS quali server sono autorizzati a inviare email a nome del dominio.

DKIM (DomainKeys Identified Mail): Serve a garantire l'integrità e l'autenticità del contenuto di un'email mediante la firma digitale.
Il mittente firma digitalmente il contenuto dell'email con una chiave privata, e il destinatario può verificare l'autenticità utilizzando la chiave pubblica associata.

DMARC (Domain-based Message Authentication, Reporting and Conformance): Fornisce un meccanismo per l'autenticazione degli email e specificare come le email non autenticate dovrebbero essere gestite. DMARC unisce SPF e DKIM, richiedendo che entrambi siano autenticati correttamente o che nessuno dei due sia superato. Consente di specificare le azioni da intraprendere per le email che non superano l'autenticazione, ad esempio, possono essere contrassegnate come spam o rifiutate.


Messaggio originale

ID messaggio	<0102018c6c93f2fe-691e3835-6ee5-472a-b956-42daaedd51eb-000000@eu-west-1.amazonses.com>
Creato alle:	15 dicembre 2023 alle ore 09:24 (consegnato dopo 0 secondi)
Da:	"Amazon.it" <promotion-it@amazon.it>
A:	sergio29b01@gmail.com
Oggetto:	Ultima occasione: Crea una Lista degli acquisti e ottieni 5€
SPF:	PASS con l'IP 54.240.0.80 Ulteriori informazioni
DKIM:	'PASS' con il dominio amazon.it Ulteriori informazioni
DMARC:	'PASS' Ulteriori informazioni

Scarica messaggio originale

Copia negli appunti

PHISHING CONTROLLATO

Dopo essermi messo d'accordo con il direttore, metteremo alla prova i dipendenti mandando loro una mail di phishing creata da noi per vedere se hanno capito la spiegazione. Invieremo loro una mail dove la loro stessa azienda offre loro un buono per la vacanza di 1000 euro, useremo una mail quasi uguale a quella aziendale ovvero Epicodesecurity@semofort.com (la differenza con quella reale si ha solo nella parte finale del dominio). Nella mail ci sara un link che riconduca sulla pagina copiata di un sito che organizza viaggi, in questo caso "evaneos", ad occhio il sito sembrerà originale ma non lo è, poiché se si guarda l'url del sito copiato da noi si nota che non è sicuro. Nel sito troveranno un link dove inserire i propri dati bancari per ricevere il bonus, ovviamente non riceveranno alcun bonus ma verranno derubati dei loro dati. L'obiettivo di questo test è far capire ai dipendenti come verificare la provenienza di una mail, infatti controllando la mail tramite "Mostra originale" capiranno che non si ha l'autorizzazione dell' SPF né tanto meno quella di DKIM e DMARC. Ovviamente nessuno verrà derubato in questo caso dato che la mail e il sito li abbiamo creati noi, questi test servono molto a cambiare la mentalità delle persone e ad evitare per quanto possibile attacchi di questo tipo da parte dei criminali informatici.