Progetto Settimana 3

SPIEGAZIONE PHISHING:

Il phishing è un tipo di attacco di ingegneria sociale, tra i più diffusi.

Il phishing consiste nell'invio di e-mail o messaggi ingannevoli che cercano di indurre le persone a rivelare informazioni preziose come password, nomi utente.

Questo tipo di attacco si basa sull'ingannare la persona, facendole credere che l'e-mail ricevuta sia stata veramente spedita da una fonte affidabile.

Le e-mail di phishing presentano diverse caratteristiche:

- La maggior parte delle e-mail ricevute provengono da fonti come banche o servizi internet con le quali la persona potrebbe avere una relazione.
- Sono presenti loghi ufficiali e testi che incitano a compiere azioni come cliccare su un link, inserire le proprie credenziali o scaricare allegati.

Una volta che una vittima esegue una di queste istruzioni, l'attaccante avrà accesso ad informazioni sensibili come credenziali o altri dati personali.

COME NON CADERE NEL PHISHING:

Per fare in modo che i dipendenti non cadano nel phishing bisogna renderli consapevoli dell'esistenza di questa minaccia.

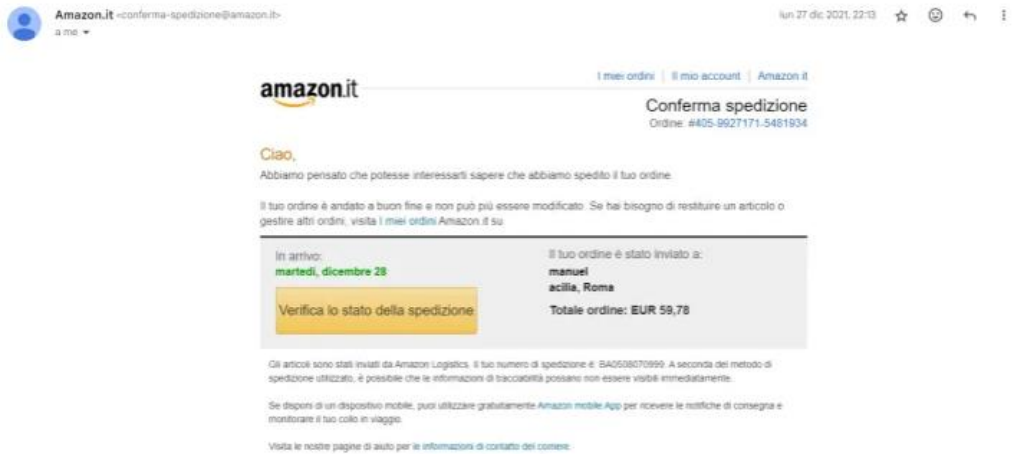
Ci sono diversi parametri da controllare per verificare l'autenticità della e-mail ricevuta:

- Spesso le e-mail ricevute presentano diversi errori di ortografia.
- L'indirizzo e-mail è sospetto, ovvero scritto in modo particolare
- Richiesta di inserire dati sensibili come nome utente e password -> per qualsiasi dubbio, dopo aver ricevuto una e-mail sospetta da un'azienda (con la quale abbiamo una relazione, per esempio una banca), conviene contattare direttamente l'azienda in questione per verificare eventuali anomalie.

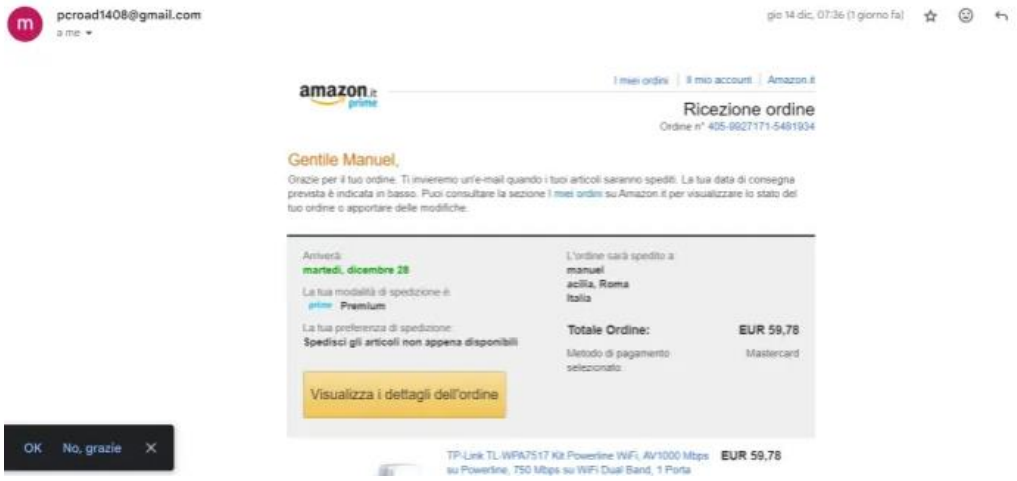
Importante per non cadere nel phishing è controllare i filtri SPF, DKIM e DMARC.

Prima di verificare questi filtri prendiamo in esempio queste due e-mail:

E-mail Originale:



E-mail di Phishing:



A prima vista queste due e-mail sembrano esattamente uguali ed è proprio per questo che è facile cadere nel phishing.

Ma facendo attenzione ci sono delle irregolarità nella seconda e-mail:

- L'indirizzo e-mail del mittente è strano, dato che stiamo parlando di una mail di Amazon non ci aspetteremmo un indirizzo scritto in questo modo.

Ora torniamo al discorso dei filtri.

I filtri che dobbiamo controllare, come detto, sono:

- SPF -> questo filtro mi permette di verificare che l'indirizzo IP che invia l'e-mail sia autorizzato a farlo per quel dominio specificato
- DKIM -> garantisce l'autenticità del contenuto dell'e-mail tramite la firma digitale.
- DMARC -> questo filtro unisce i filtri precedenti in modo che siano entrambi autenticati.
- La scritta "PASS" dopo ognuno di questi filtri.

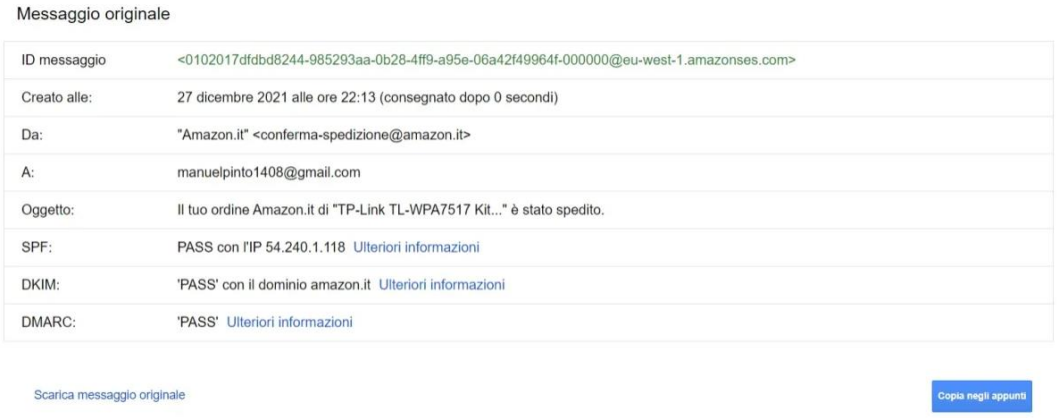
Ma come li controlliamo questi filtri?

Clicchiamo sull'e-mail che ci interessa e successivamente sui tre puntini accanto alla freccetta per rispondere all'email.

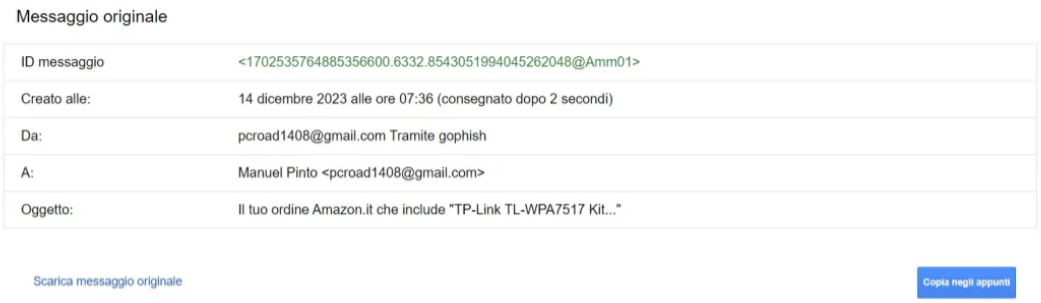
Successivamente clicchiamo su "mostra originale".

Dopo aver cliccato verremo portati in ina pagina dove potremo vedere il codice originale dell'e-mail.

E-mail vera



E-mail sospetta:



Come si può notare nell'email vera i filtri sopracitati sono tutti seguiti dalla scritta PASS, nel filtro SPF vediamo l'IP autorizzato all'invio dell'e-mail, mentre alla voce DKIM vediamo il dominio registrato, in questo caso amazon.it.

La seconda e-mail, invece, quella sospetta, non presenta nessuno di questi filtri. La mancanza di questi filtri ci fa capire che siamo di fronte a un e-mail non originale e quindi pericolosa.

COME CREARE UN ATTACCO DI PHISHING

Esistono diversi programmi per effettuare attacchi di phishing, uno di questi è gophish.

Per poter effettuare questo attacco prenderei una mail che capita spesso di ricevere, come per esempio le e-mail di una banca o di Amazon.

Cerco un'e-mail che voglio copiare.

Nella schermata che mi appare dopo aver cliccato "mostra originale", mi copio il codice dell'e-mail ricevuta.

Copio il codice su gophish in modo che mi ricrei la stessa e-mail identica.

Invio l'e-mail, tramite gophish sarò poi in grado di verificare quanti click ha ricevuto il link malevolo che ho inserito nell'email, e in base al malware che ho voluto diffondere potrò poi agire di conseguenza, per esempio se ho ricreato l'email di una banca richiedendo l'accesso dell'utente, ora sarò in grado di visualizzare le sue credeniali.