PROGETTO S3/L5

Obiettivo: lo scopo del progetto è,spiegare e informare i dipendenti dell'azienda Epicodesecurity che ha un sito web suo(www.Epicodesecurity.it),un server email con l'email aziendale Epicodesecurity@semoforti.com, sui i rischi di attachi di ingegneria sociale,in particolare modo il phishing .

1-capire che cos'è l'ingegneria sociale

L'ingegneria sociale: è una forma di manipolazione psicologica in cui gli attaccanti cercano di ottenere informazione sensibili o indure le persone a compiere determinate azioni attraverso l'inganno,la manipulazione e l'uso delle relazioni umane.

Quali informazioni vengono utilizzate a dei fini malevoli come: rubare soldi sulla carta di credito , o per accedere ad altri informazioni più sensibile etc...

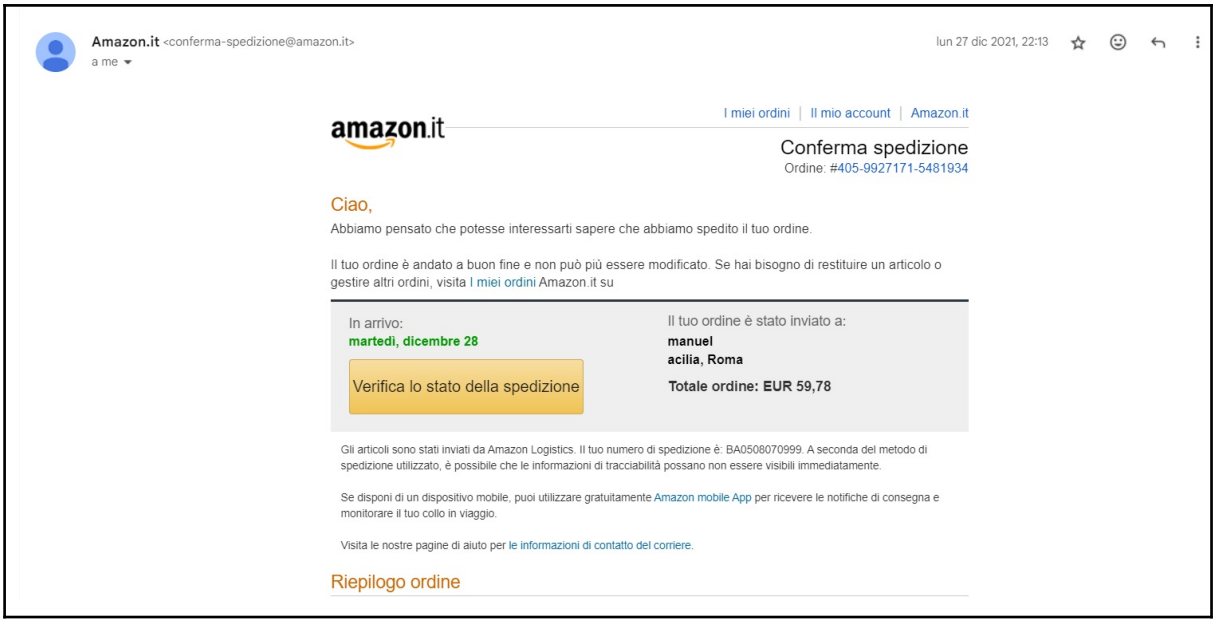
Ci sono vari attacchi di ingegneria sociale,ma vedremo uno in particolare: "il phishing" .

2- che cos'è il phising ?

Il phishing è uno tra i vari attachi di ingegneria sociale; è uno tra i più diffusi e pericolosi.Coinvolge l'invio di messaggi,generalmente e-mail,che sembrano provenire da fonti affidabili per indurre le persone a rivelare informazioni sensibii come:password o dettagli finanziari.

3- cosa devono vedere, in particolare i dipendenti per non cadere nel phishing?

PROGETTO S3/L5



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

lun 27 dic 2021, 22:13

amazon.it

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

Per capire cosa deve fare un dipendente per non cadere nel phishing uso l'imagine sopra che dimostra la sottigliezza di una mail di phishing . Come possiamo vedere questa imagine sembra essere una mail mandata da Amazon ma non è il caso.questa mail est un phishing.

-Generalmente la prima cosa da fare è quello che sto faccendo adesso ovvero informare i dipendenti. Peché molti dipendenti non sono consapevoli che esistono questi tipi di attacchi o delle tattiche utilizzate dagli attaccanti.
-Evitare di fare clic su link presenti nelle e-mail sospette o provenienti da mittenti non riconosciuti. Invece, verificare manualmente l'URL visitando direttamente il sito web dell'organizzazione, se necessario.

- stare attento alle richieste di fornire informazioni sensibili, come password o dettagli di carte di credito, tramite e-mail o altri mezzi di comunicazione online. Le organizzazioni legittime di solito non richiedono tali informazioni in questo modo.
-non lasciarsi ingannare con i login dei siti.generalmente una volta che gli utenti vedono che i login dei siti sono giusto cliccano sopra; e questo è pericoloso ,perché i phishing sono siti clonati e quindi assomigliano quelli originali.

PROGETTO S3/L5

4-creazione di un phishing controllato.

Se devo creare un mail di phishing , la prima cosa da fare è cercare il massimo di informazione possibile sulla persona a chi è destinato la mail di phishing; avendo quelli informazioni vado su un sito sul quale ha l'habitudine di andare; clono quel sito usando l'Applicazione gophish e mando il link del sito clonato al destinatario e un volta che clicchera sul quel link i giocchi saranno fatti.