I rischi connessi a una minaccia basata sull'ingegneria sociale, in particolare il phishing, che mira a ottenere informazioni sensibili, sono significativi. Il furto di identità rappresenta uno dei pericoli principali, poiché dati personali, finanziari e credenziali di accesso possono essere compromessi. Gli attacchi di phishing possono risultare in accessi non autorizzati a sistemi e reti, con il conseguente rischio di perdite finanziarie sia per individui che per aziende. In aggiunta, si possono diffondere  malware attraverso i messaggi di phishing  che vanno a minacciare la sicurezza dei sistemi.
Il phishing è un attacco basato sull'ingegneria sociale che spesso coinvolge la creazione di messaggi non legittimi, come e-mail o chiamate, al fine di indurre le vittime a rivelare dati personali o a compiere azioni non autorizzate. Per ciò va sottolineata l'importanza della consapevolezza e della formazione per difendersi da questa tipologia attacchi.

Dopo aver sottolineato l'importanza della conoscenza, procediamo con la formazione dei dipendenti con un corso formativo della durata complessiva di 6 ore:

Ore 9:00 - 10:00: Breve introduzione a Kevin D. Mitnick e alle minacce di phishing

Ore 10:00 - 12:00: Principi di ingegneria sociale: come gli attaccanti manipolano le persone

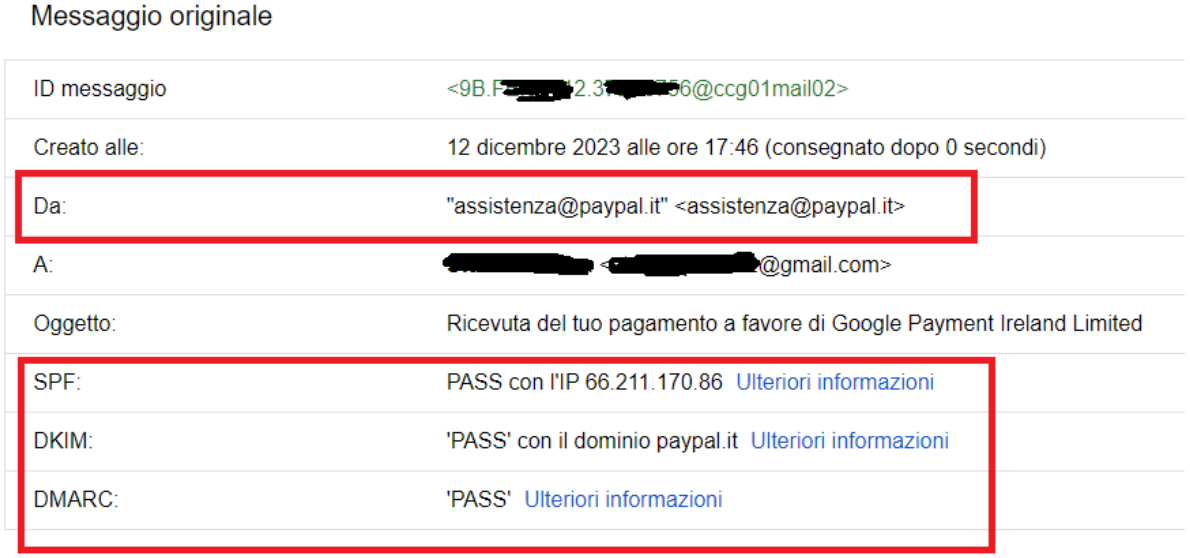
Ore 12:00 - 13:00: Pausa pranzo

Ore 13:00 - 14:00: Analisi di casi di phishing reali e tecniche per identificare segnali sospetti

Ore 14:00 - 16:00: Simulazioni di phishing per riconoscere e gestire attacchi

Obiettivo del Corso:
Comprendere le tecniche di ingegneria sociale utilizzate nel phishing e sviluppare competenze per riconoscere e gestire mail di phishing.

Per verificare la veridicità di una mail si devono controllare i seguenti parametri:



Il dominio da cui è stata inviata è "assistenza@paypal.it"...
E per ultimo verificare che SPF, DKIM e DMARC abbiano il PASS cioè la verifica della firma digitale e dell’autenticità del messaggio.

Con il permesso del direttore dell’azienda di creare phishing controllato inizio pianificando i target. Progetto e invio email di phishing simili a quelle legittime integrate con elementi ingannevoli come link a pagine di login false o allegati dannosi. Ad esempio dopo aver verificato le informazioni pubbliche di figure autorizzate in modo da impersonarle posso inviare delle email con tanto di pdf con script incorporati al reparto contabilità in modo che controllino e verifichino eventuali errori. Successivamente passo a monitorare le loro risposte e azioni e una volta terminato raccolgo i dati e fornisco un feedback con tanto di misure consigliate per migliorare la sicurezza dell'azienda.