EPICODE

**S5L5**

Esempio E-Mail Phishinglinea orizzontale

# 

# Introduzione

Come progetto oggi, andremo ad analizzare un contesto di E-mail phishing, in particolar modo come vengono rubati dati intimi del cliente. In questo caso, come esempio, ho scelto il furto di dati intimi di un cliente di una determinata banca (che ho descritto nelle varie foto che andremo ad analizzare in seguito).

**ANALISI DELLA E-MAIL**

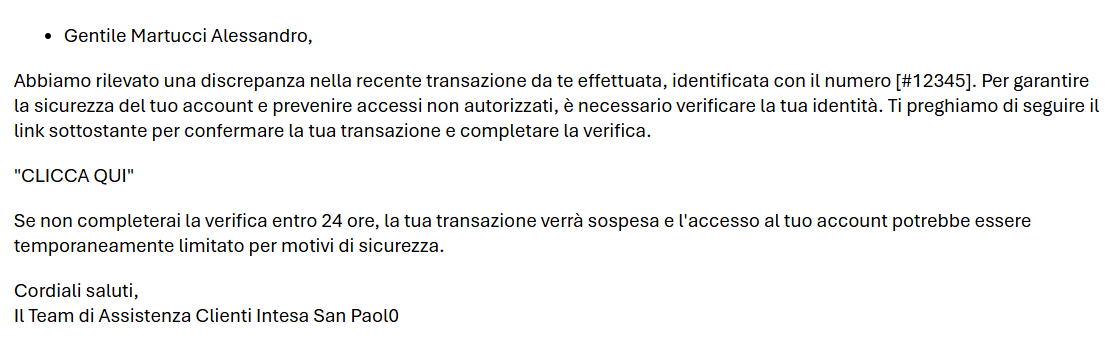


Come possiamo ben vedere, l’e-mail in questione sembrerebbe essere perfetta, ma ci sono alcuni dettagli ed errori che fan sì che sia sospetta, è quindi di non fidarsi. Il primo dettaglio è il **“-”** tra le due parole dopo la **“@”**. Di solito, come e-mail verificata, non si utilizza mai il trattino alto o basso, quindi, in questo caso, è il primo errore che ci tiene in allerta dal non fidarci. Come secondo errore, anche se è difficile notarlo nella lettura veloce, abbiamo lo **“0”** al posto di una **“o”**, nella parola **“sanpaolo”** altro errore non da poco che ci fa capire che l’e-mail non è verificata. In ogni caso, quando si ricevono e-mail del genere, è sempre corretto prevenire la sicurezza, e quindi di andare ad informarsi nel sito della propria banca se l’e-mail ricevuta è quella verificata dalla banca. Inoltre, ci sono dei tool di estensione che

se utilizzati ci accertano se quella e-mail è verificata oppure un e-mail phishing.



Quando avviamo una transazione, nelle varie informazioni abbiamo anche il numero della transazione (come vediamo sopra nell’esempio), ed è bene quindi verificare anche il numero, prima di cliccare in qualche link sospetto dell’e-mail. Di solito e-mail phishing utilizzano numeri banali (come sopra indicato), ma non è sempre detto.



Quando riceviamo e-mail sospette, il contenuto in esse è totalmente simile che non riusciamo a capire dove ci sia l’errore che ci metta in allerta, ma andiamo a prendere in questione alcune “Leggi” non scritte che ci possono far capire molto su l’e-mail in esempio. Per prima cosa, nessuna banca vi chiederà di inserire i vostri dati sensibili su un link, soprattutto se ricevuto via e-mail. Per qualunque informazione, la banca si appresta ad utilizzare l’applicazione mobile o il sito ufficiale. Il secondo punto è riguardante la limitazione dell’account, cosa da non prendere alla leggere, visto che per qualunque limitazione o blocco del conto corrente, la banca vi avvertirà tramite una chiamata. Il terzo punto è il link. Determinati link hanno banali errori che ci fanno capire di essere dei Phishing **( https://www.intesasanpa0l0.com/ )**, quindi da non cliccare se non si vogliono problemi come malware o furto di dati. Il quarto punto sono i vari errori che troviamo nell’e-mail, come ad esempio **“San Paol0”** dove ha uno zero al posto della **“o”**, dove ci fa capire che l’e-mail in questione non è verificata.