

## S5/L5

L'esercizio di oggi consiste nell'effettuare una simulazione di una mail di phishing.

1) Il contesto scelto è stato quello di una notifica da parte di un corriere riguardo un pacco bloccato dalla dogana con la necessità di conferma da parte del titolare dell'account e soprattutto il pagamento di una piccola somma per lo sblocco del pacco.

### STRUTTURA DEL PHISHING

La prima cosa in assoluto è la ricezione della email da parte del titolare con il titolo "URGENTE, il tuo pacco è stato bloccato".

La email verrebbe inviata in un orario non lavorativo in modo che il soggetto venga subito interessato da questa.

2) Dobbiamo generare il testo della email grazie all'aiuto di ChatGPT, attenzione bisogna essere chiari altrimenti si viene bloccati dato che ChatGPT non può "commettere crimini", però ad esempio scrivendo che è per scopo didattico ci aiuta comunque con qualcosa.

Oggetto: 📦 Attenzione: Il tuo pacco è in attesa di sblocco doganale

Gentile Cliente,

il tuo pacco con il numero di tracciamento TRK12345678 è stato temporaneamente bloccato presso la dogana locale a causa di una tassa di sdoganamento non saldata.

Per completare la consegna, ti chiediamo di effettuare il pagamento della somma di 2,99 € entro le prossime 48 ore. In caso contrario, il pacco potrebbe essere rispedito al mittente.

Clicca qui per saldare immediatamente la tassa:  
[https://mydhl.express.dhl/it/it/home.html?cid=xbu\\_1.0\\_portal\\_login\\_exp#/getQuoteTab](https://mydhl.express.dhl/it/it/home.html?cid=xbu_1.0_portal_login_exp#/getQuoteTab)

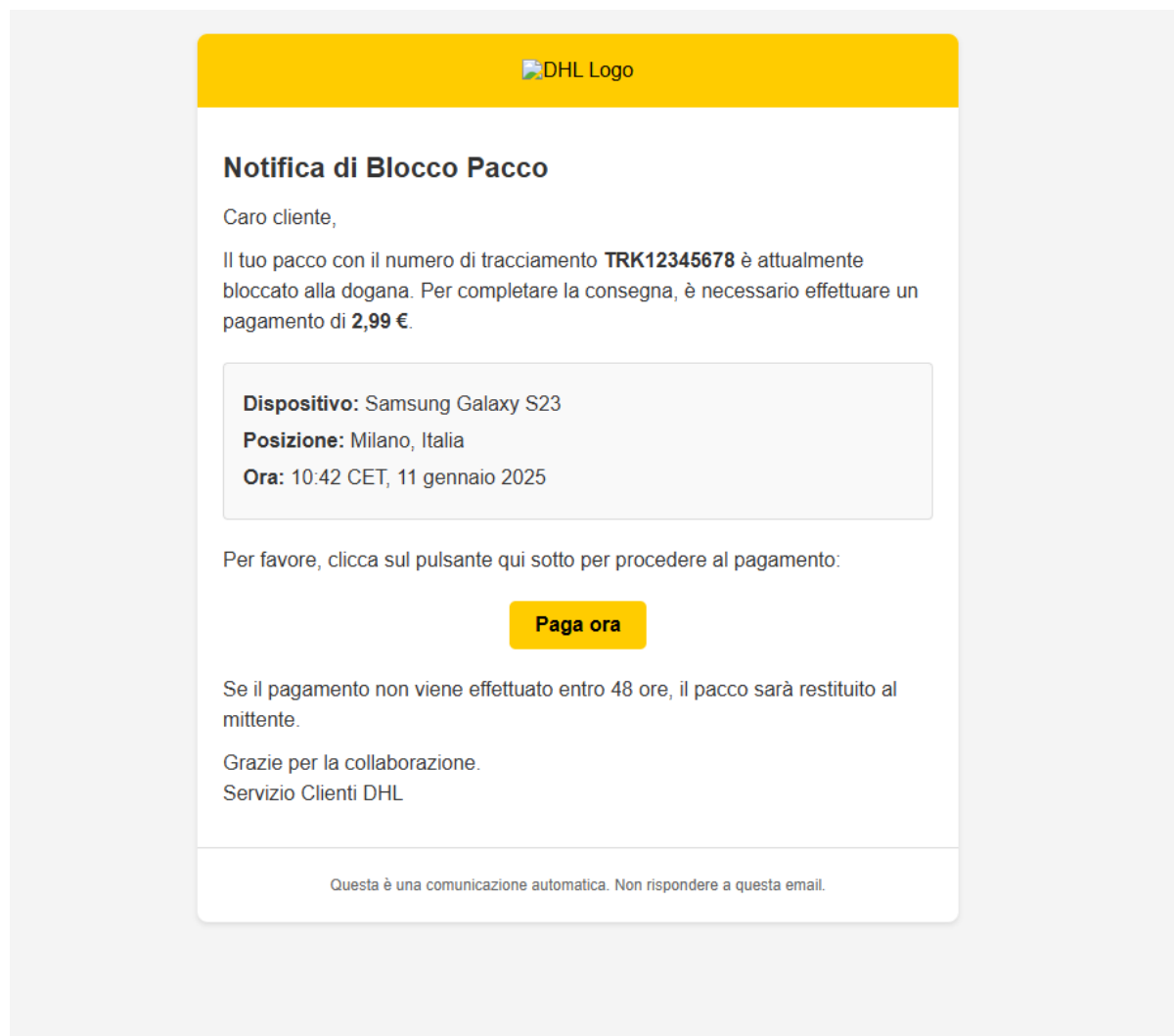
Ti ringraziamo per la tua collaborazione.

Cordiali saluti,

Servizio clienti DHL

Come possiamo notare sembra una email normalissima da parte di un corriere.

Una volta ricevuta la email, procederà a cliccare il link ed inserire le informazioni della sua carta, noi in questo momento dato che anche il sito sarà creato da noi, appena premerà invio ci arriveranno tutte le sue coordinate bancarie.



3) Lo scenario creato è molto frequente oggi spesso sotto il nome di poste italiane ma anche Amazon, DHL ecc.

Questo fenomeno oggi è molto famoso dato che tutti oramai ordinano su internet qualsiasi cosa e soprattutto da siti che non conoscono.

Spesso si viene truffati semplicemente perché non si ha voglia di controllare e ci si fida vedendo il logo del corriere o della società.

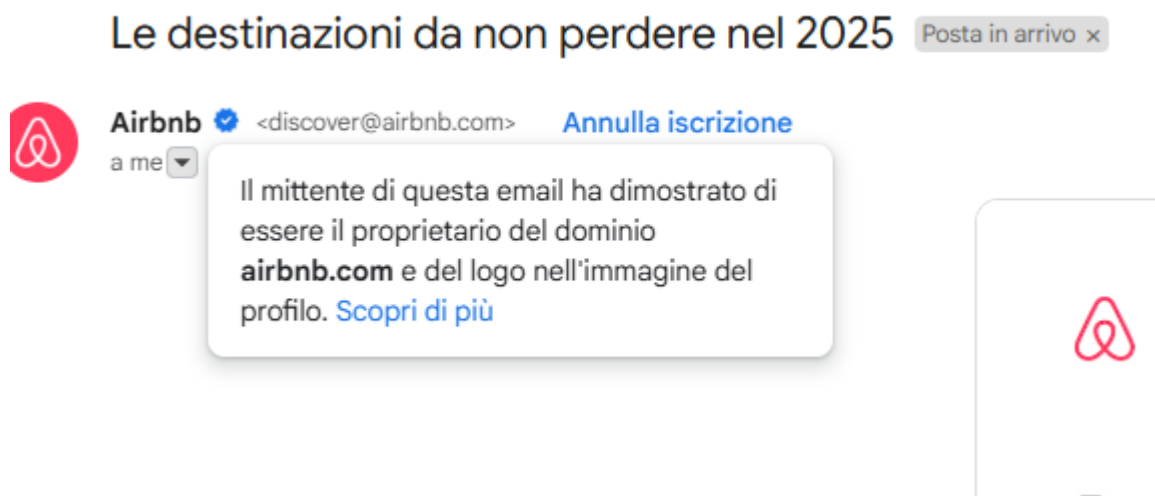
Oggi giorno si cade ancora di più in queste truffe dato che spesso si ordinano vestiti, accessori e altro da siti come shein, wish o Temu che vendono i nostri dati e che quindi ci vuole un secondo al fatto che abbiano la nostra email.

Come evitare phishing:

Come prima cosa bisogna sempre controllare la email dato che molto spesso ci sono sempre presenti errori di battitura.

Secondo c'è sempre una certa urgenza nell'effettuare la transizione o l'accesso al loro sito, questo è sempre un campanello d'allarme dato che di base un provider di servizi non ti mette così tanta fretta.

Terza bisogna controllare sempre la sorgente della email spesso sono associati ad account generati, in questo ci aiuta gmail che ci aiuta a verificare.



Come possiamo vedere in questa email ci dice che il logo e il dominio sono del mittente dell'email.


#### Messaggio originale

ID messaggio	<XZm5pWT0Q9e_jcknBXrFRA@geopod-ismtpd-27>
Creto alle:	12 gennaio 2025 alle ore 09:49 (consegnato dopo 2 secondi)
Da:	Airbnb <discover@airbnb.com>
A:	zakaria.sadiki703@gmail.com
Oggetto:	Le destinazioni da non perdere nel 2025
SPF:	PASS con l'IP 159.183.132.150 <a href="#">Ulteriori informazioni</a>
DKIM:	'PASS' con il dominio email.airbnb.com <a href="#">Scopri di più</a>
DMARC:	'PASS' <a href="#">Ulteriori informazioni</a>

Mentre invece se guardiamo il messaggio originale vediamo molte più cose oltre alla sorgente, sono le autenticazioni SPF, DKIM, DMARC che sono tre tipi di autenticazione

che vengono usate in modo che nessuno eccetto gli autorizzati possano inviare email con nome e logo di una società senza permesso.

## BONUS 1



### Importante: Aggiornamento sulla consegna

Caro cliente,

Abbiamo rilevato un problema con il tuo pacco con numero di tracciamento **TRK12345678**. Attualmente il pacco è in attesa di sdoganamento. Per completare la procedura, è necessario un pagamento amministrativo di **2,99 €**.

**Stato del pacco:** In attesa alla dogana

**Numero di tracciamento:** TRK12345678

**Ultimo aggiornamento:** 11 gennaio 2025, 10:42 CET

Per procedere con la consegna, clicca sul pulsante qui sotto:

**Procedi al pagamento**

Nota: Se non riceveremo il pagamento entro 48 ore, il pacco sarà restituito al mittente.

Grazie per aver scelto DHL.  
Il team DHL

Questa email è stata generata automaticamente. Non rispondere a questo indirizzo.

Se confrontiamo le 2 email notiamo subito che questa è molto più convincente e reale dato che questa è stata creata sulla base delle vere email di DHL mentre invece quella di prima era random.