Contesto realistico

Un destinatario riceve un'email che sembra provenire da un noto servizio di spedizioni. L'email informa della necessità di confermare il pagamento di una piccola tassa per completare la consegna di un pacco in arrivo. L'obiettivo del phishing è ottenere dati della **carta di credito** o altre **informazioni finanziarie**.

I truffatori sfruttano situazioni comuni, come la consegna di pacchi, per creare email di phishing convincenti. Con l'aumento degli acquisti online, è normale aspettarsi notifiche da corrieri come **DHL**, **UPS** o Poste **Italiane**.

Email di phishing

Oggetto: 📦 Attenzione: Consegna sospesa - Azione richiesta

Mittente: **notifiche@expressdelivery-it.com**

Testo dell'email:

Gentile Mario Rossi,

Ti informiamo che il tuo pacco n. EXP562487789IT è stato trattenuto presso il nostro centro di smistamento a causa di una tassa di consegna non saldata di €2,99.

Per completare la consegna, ti chiediamo gentilmente di effettuare il pagamento entro 24 ore. Puoi procedere cliccando sul seguente link:

Conferma il pagamento

Se il pagamento non verrà effettuato entro il termine indicato, il pacco verrà restituito al mittente.

Grazie per aver scelto .

Cordiali saluti,
Team Supporto Clienti
ExpressDelivery Italia

Nota: Per ulteriori informazioni, contattare il nostro servizio clienti al numero **+39 0123 987654**.

Spiegazione dello scenario

E’ frequente ricevere email dai corrieri per aggiornamenti sulle spedizioni, l'importo richiesto (€2,99) è così modesto da sembrare plausibile e induce meno sospetti, l'email include un numero di pacco falso ma verosimile per aumentare la credibilità, il tono è simile a quello usato dai veri corrieri nelle loro comunicazioni ufficiali.

Elementi sospetti

L'indirizzo del mittente e il dominio del link non corrispondono a quelli ufficiali di un noto corriere. La richiesta di pagamento tramite link poiché i corrieri autentici raramente richiedono pagamenti urgenti via email senza offrire alternative chiare o verificabili. L’urgenza forzata, il termine di 24 ore è una tattica comune nei tentativi di phishing per creare pressione sulla vittima.

Raccomandazione

Controllare sempre l'autenticità del mittente e del link senza cliccare. Visitare il sito ufficiale del corriere digitando manualmente nel browser per verificare eventuali problemi con la consegna. Contattare il servizio clienti del corriere utilizzando i numeri ufficiali presenti sul sito legittimo.