Phishing

Il phishing è la pratica di social engineering di inviare e-mail o altri messaggi che sembrano provenire da aziende rispettabili al fine di indurre le persone a rivelare informazioni personali, come credenziali, numeri di carte di credito o altri dati sensibili.

Caso studio: finta notifica di spedizione da parte di un noto corriere

Effettuare acquisti on line è una pratica estremamente diffusa nel mondo odierno, dove sempre più persone si trovano spesso a gestire e monitorare la consegne dei propri pacchi. Questo contesto crea molteplici opportunità per truffatori intenzionati a sfruttare il fenomeno delle spedizioni per perpetrare attacchi di phishing, dove messaggi e mail fraudolenti vengono scritti per sembrare notifiche di spedizione.

Il phishing sfrutta inoltre la pratica di inviare spam a un vastissimo pubblico, aumentando così la probabilità che le loro comunicazioni raggiungano persone che sono effettivamente in attesa di un pacco.

Testo della mail fraudolenta

Oggetto: URGENTE: Il tuo pacco è stato trattenuto. Azione richiesta per la consegna

---

Gentile Cliente,

Siamo spiacenti di informarti che non siamo riusciti a consegnare il tuo pacco [ID spedizione: 098123654] a causa di informazioni incomplete o errate fornite durante la spedizione. Per garantire che il pacco arrivi a destinazione, ti chiediamo di aggiornare le tue informazioni **entro 48 ore**.

Puoi farlo cliccando sul link sottostante:

www.spedizione-aggiorna.com

Se non aggiorni le informazioni entro il tempo indicato, il pacco verrà restituito al mittente e potrebbero essere applicate **penali aggiuntive** per il mancato ritiro.

Grazie per la collaborazione. Se hai bisogno di assistenza, il nostro servizio clienti è a tua disposizione.

Cordiali saluti,
Il team di supporto DHL
support@dhl-consegna.com

Analisi della mail

La mail di phishing presa in esame è progettata per apparire come una comunicazione da parte del conosciuto corriere DHL. Il messaggio informa il destinatario che ci sono problemi con la consegna di un pacco e richiede l'aggiornamento delle informazioni di spedizione tramite un link esterno. Come già menzionato, questo tipo di phishing può sfruttare la curiosità del destinatario o il fatto che questo possa essere effettivamente in attesa della consegna di un pacco, rendendolo vulnerabile a una comunicazione che sembra provenire da una fonte affidabile.

In questo particolare esempio, possiamo vedere alcuni elementi che rendono la mail fraudolenta credibile:

1. Eventuale tempistica: se il destinatatrio ha recentemente ordinato un prodotto e si aspetta una consegna, il ricevere una notifica dal corriere può sembrare normale o addirittura previsto, rendendo probabile il fatto che il destinatario non sospetti una frode.
2. Dettagli specifici: la mail contiene un presunto "ID spedizione", dando l'illusione di autenticità nonostante sia generico e non corrisponda ad alcun numero reale.
3. Logo e scrittura professionale: gli attaccanti potrebbero utilizzare il logo del corriere e un linguaggio formale per rendere la mail più convincente, copiando lo stile delle comunicazioni ufficiali, anche se molto spesso sono presenti errori di grammatica e ortografia.

Allo stesso tempo sono presenti elementi che si possono considerare tipici di una mail di phishing:

1. Link sospetto: anche se l'URL sembra plausibile non appartiene al dominio ufficiale del corriere. I link falsi spesso sono creati per assomigliare a quelli legittimi, ma differiscono in piccoli dettagli, come in questo caso la mancanza del dominio di DHL.
2. Indirizzo mail del mittente: "support@dhl-consegna.com" è diverso dall'indirizzo ufficiale che dovrebbe essere utilizzato da DHL. Come per i link, spesso le email di phishing contengono domini simili a quelli reali ma con lievi differenze.
3. Richiesta di aggiornare i dati personali: la richiesta di aggiornamento dati personali tramite mail, soprattutto se riguarda informazioni finanziarie, non viene in genere effettuata tramite link forniti via mail, bensì tramite il sito ufficiale.
4. Minaccia di penalità: le mail di phishing creano spesso un senso di urgenza minacciando conseguenze facendo leva sul timore del destinatario di incorrere in una sanzione se questo non agisce in modo tempestivo, come in questo caso la penale per mancato ritiro.

L'obiettivo di questa mail è in sostanza quello di indurre il destinatario a cliccare sul link, di modo da reindirizzarlo ad un sito fraudolento creato dal mittente che invita la vittima ad inserire i propri dati. In base al tipo di informazioni richieste, il mittente della mail può avere accesso a credenziali, dati finanziari e altre informazioni sensibili della vittima.