Il Phishing della Consegna Fantasma

Con l’aumento degli acquisti online, gli attacchi di phishing si adattano ai comportamenti digitali quotidiani. Una tecnica efficace simula la mancata consegna di un pacco, sfruttando urgenza e abitudini dell’utente. Questo schema, semplice ma studiato, impiega link e QR code per sottrarre dati sensibili.

Oggetto: Tentativo di consegna fallito – azione richiesta entro 24h
Mittente: notifiche@dhl-servizi.com
Reply-To: noreply@dhl.com

Contenuto dell'email di phishing:

Gentile cliente,

Non siamo riusciti a consegnare il tuo pacco in data 01/05/2025.
Il corriere non ha trovato nessuno al momento della consegna.

Codice spedizione: 2483-IT-7810
Destinatario: [Cognome, Nome]
Indirizzo: [Parzialmente oscurato per privacy]

Per riprogrammare la consegna:

1. Scansiona il codice QR con il tuo smartphone
oppure
2. Clicca qui per scegliere data e fascia oraria

Riprogramma consegna

QR code allegato (simulato):

Nota: Se non confermi entro 24 ore, il pacco verrà restituito al mittente.
Non rispondere a questa email: è un messaggio automatico.

DHL Express Italy
Servizi Clienti Automatici

L'email di phishing creata simula una comunicazione da parte di una compagnia di spedizioni, come DHL, per informare il destinatario di un tentativo di consegna fallito. Il messaggio fittizio invita il destinatario a scansionare un QR code o cliccare su un link per riprogrammare la consegna del pacco. L'email sembra autentica, grazie all'uso di un mittente che imita l'indirizzo di un'azienda nota, e contiene dettagli che rendono il messaggio verosimile, come il numero di spedizione e un riferimento al corriere.

Gli attacchi di phishing basati su una notifica di pacco non consegnato sono costruiti attorno all'idea di una comunicazione urgente da parte di un corriere, come DHL o un altro servizio di spedizione. La logica dietro questo attacco si fonda sulla preoccupazione naturale che una persona potrebbe avere nel ricevere un avviso di mancata consegna di un pacco importante. Molte persone, infatti, potrebbero trovarsi nella situazione di aspettare una consegna (sia essa personale olegata a un acquisto online), e questo aumenta la probabilità di interazione con il messaggio.
Le persone sono più propense ad agire impulsivamente quando sentono che una loro azione è necessaria per evitare un problema imminente, come la perdita di un pacco o la mancata ricezione di un prodotto acquistato.

Punti di Realismo:

1. **Utilizzo del QR Code:**

Un elemento distintivo di questa email di phishing è l'inclusione di un QR code. Il QR code è una tecnologia che consente agli utenti di scansionare un codice tramite un dispositivo mobile per accedere rapidamente a un sito web. Poiché i QR code sono molto comuni oggi, specialmente nelle transazioni quotidiane (come pagamenti e accesso a informazioni), l'inclusione di questo elemento
aumenta l'affidabilità dell'email. La vittima potrebbe essere più propensa a interagire con il codice senza sospetti.

Quando il QR code viene scansionato, il dispositivo mobile dell'utente apre un link fittizio che imita il sito web di DHL, ma in realtà si tratta di un sito di phishing. Questo sito potrebbe chiedere alla vittima di inserire informazioni sensibili come nome, indirizzo, numero di carta di credito, o altre credenziali.

2. **Uso di marchi noti:**

Il logo e i colori di aziende come DHL, UPS, o Poste Italiane vengono replicati per aumentare la fiducia dell'utente.

3. **Linguaggio professionale:**

Il testo può essere ben scritto, con tono formale, sintassi corretta e formule standard (es. "Gentile cliente", "La informiamo che…").

4. **Dati verosimili:**

L'email può includere un numero di tracciamento fittizio, un indirizzo o una fascia oraria che sembrano plausibili.

5. **QR code o link "funzionali":**

Viene incluso un QR code che sembra rimandare a un tracciamento rapido della spedizione, simulando pratiche comuni delle vere aziende logistiche.

6. **Firma e contatti realistici:**

L'email può terminare con il nome di un operatore clienti e riferimenti aziendali credibili (es. "Servizio Clienti DHL Express").

Indicatori sospetti di Phishing:

1. **Indirizzo email del mittente:**

Spesso, dietro un nome apparentemente ufficiale, si nasconde un dominio non coerente (es. dhl@trackdelivery-update.net invece di @dhl.com).

2. **Link o QR code non verificabili:**

Il QR code porta a un URL sospetto, non coerente con il sito ufficiale (es. dhl-secure.delivery-info.cc). I link reali vanno sempre verificati prima di cliccare.

3. **Richiesta di dati personali o pagamento:**

Un vero corriere non chiede dati sensibili o pagamenti via email per completare la consegna.

4. **Errori minimi di grammatica o formattazione:**

Anche quando l'italiano è corretto, possono esserci dettagli fuori posto (spaziature irregolari, maiuscole forzate, simboli strani).

5. **Assenza di personalizzazione:**

L'email si rivolge al "cliente" in modo generico, senza indicare il nome o altri dettagli specifici.