Antonio Podda S5L5 Simulazione di una mail phishing

Oggetto: Consegna pacco bloccata in dogana – Azione richiesta

Mittente: notifiche@sda-express.com *(falso dominio, somigliante a quello reale)*

Testo dell'email:

Gentile Cliente,

Ti informiamo che il tuo pacco con numero di tracking 8DD497h23 è attualmente bloccato in dogana. Per procedere alla consegna, è richiesto il pagamento di una tassa doganale pari a $2,99.

Ti invitiamo a confermare i dettagli del pagamento e le tue credenziali entro 24 ore cliccando sul link sottostante:

Sblocca il tuo pacco ora

Se non effettui questa operazione entro il termine indicato, il pacco sarà restituito al mittente.

Grazie per aver scelto SDA,
Il Team di Assistenza SDA

Scenario Creato

In questo scenario, un utente riceve un’email apparentemente inviata dall'azienda di spedizioni SDA. Il messaggio informa che un pacco destinato al destinatario è bloccato in dogana e che, per completare la consegna, è necessario effettuare un pagamento di $2,99. Inoltre, viene chiesto di inserire le proprie credenziali personali per procedere. La richiesta è accompagnata da un senso di urgenza: se non si agisce entro 24 ore, il pacco verrà restituito al mittente.

Questo scenario sfrutta la combinazione di una situazione plausibile (blocchi doganali e piccole tasse di sdoganamento) con elementi di pressione psicologica. Per chiunque abbia recentemente ordinato online, ricevere un’email di questo tipo potrebbe sembrare del tutto normale. Inoltre, l’uso di un numero di tracking specifico (ad esempio, 8DD497h23) conferisce un ulteriore tocco di credibilità, portando il destinatario a credere che l’email sia autentica.

Perché l’email potrebbe sembrare credibile alla vittima?

Un'email di phishing come questa può sembrare convincente per diversi motivi:

1. Branding familiare: L’email utilizza un nome noto come SDA, un’azienda di fiducia nel settore delle spedizioni. Questo dà immediatamente una parvenza di legittimità. La maggior parte degli utenti non si sofferma a verificare l’esattezza del dominio del mittente.
2. Contesto comune: Molti utenti effettuano ordini online o ricevono pacchi, e messaggi relativi a blocchi doganali o piccoli pagamenti sono situazioni realistiche e familiari.
3. Costo minimo: La somma richiesta è di soli $2,99, una cifra sufficientemente bassa da non destare sospetti. L’utente potrebbe pensare che il rischio sia minimo e procedere al pagamento senza riflettere.
4. Urgenza: La scadenza di 24 ore crea un senso di pressione, inducendo la vittima ad agire impulsivamente. Il tempo limitato riduce anche la possibilità di controllare l’autenticità del messaggio.

5. Numero di tracking: L’inclusione di un codice (come 8DD497h23) rende il messaggio più credibile, dando l’impressione che il pacco esista davvero e che l’azienda abbia accesso a informazioni precise.

Elementi che dovrebbero far scattare un campanello d’allarme

Nonostante l’apparente autenticità, ci sono segnali che dovrebbero mettere in guardia il destinatario:

1. Mittente sospetto: L’indirizzo email sembra legato a SDA, ma presenta leggere variazioni. Ad esempio, un mittente come *notifiche@sda-express.com* potrebbe sembrare autentico, ma differisce dal dominio ufficiale di SDA (*notifiche@sda.it*).
2. Link fraudolento: Passando il mouse sul link fornito nell’email, si potrebbe notare che reindirizza a un sito web estraneo o sospetto, diverso da quello ufficiale di SDA.
3. Richiesta di pagamento via email: Le aziende affidabili non richiedono mai pagamenti diretti tramite email. Eventuali tasse o costi sono comunicati tramite portali ufficiali.
4. Errori nel testo: Anche se minimi, le email di phishing spesso contengono errori grammaticali, di formattazione o di traduzione. Questi dettagli possono indicare che l’email non è legittima.
5. Mancanza di personalizzazione: Un’email autentica solitamente include il nome completo del destinatario. Il mancato utilizzo di dettagli personali dovrebbe insospettire.
6. Pressione psicologica: Il senso di urgenza (“rispondi entro 24 ore”) è una tecnica comune per impedire al destinatario di riflettere con calma e di verificare le informazioni.

Come difendersi

È fondamentale che gli utenti sappiano riconoscere email fraudolente come questa e adottino le seguenti misure di protezione:

1. Verifica il mittente: Controlla con attenzione l’indirizzo email. Anche una piccola variazione nel dominio può indicare un tentativo di phishing.
2. Non cliccare sui link: Evita di cliccare direttamente sui link presenti nell’email. Accedi invece al sito ufficiale dell’azienda tramite il browser e verifica lo stato del pacco inserendo il numero di tracking.
3. Controlla il numero di tracking: Inserisci il codice fornito direttamente sul sito ufficiale dell’azienda di spedizioni per verificarne la validità. Se il numero non è riconosciuto, l’email è probabilmente una truffa.
4. Segnala il messaggio: Se sospetti che un’email sia fraudolenta, inoltrala all’azienda coinvolta o al tuo reparto IT per ulteriori analisi. Questo aiuta anche a prevenire attacchi simili.
5. Formazione: Partecipa a corsi o seminari sulla sicurezza informatica per imparare a riconoscere tecniche di phishing e altre minacce.

Prevenire gli attacchi di phishing richiede attenzione e buone pratiche. Anche un piccolo errore può avere conseguenze significative, come la perdita di denaro o l’esposizione di dati sensibili.