

Pratica S5L5

L'email simula una conferma di ordine proveniente da IKEA, un'azienda ben conosciuta nel settore dell'arredamento. Il messaggio contiene informazioni tipiche che un cliente si aspetterebbe, come il numero d'ordine, i dettagli di spedizione e un riepilogo degli articoli acquistati.

Obiettivo del phishing: Indurre la vittima a cliccare sul link di tracciamento falso ("Traccia il tuo ordine") che rimanda a un sito malevolo. Questo sito potrebbe rubare le credenziali dell'utente, i dati della carta di credito o infettare il dispositivo con malware.

Oggetto:

 Conferma Ordine IKEA #56789 - Spedizione in Arrivo

Testo Email:

IKEA Italia

Gentile cliente,

Grazie per il tuo ordine con IKEA. Il tuo ordine è stato confermato ed è pronto per la spedizione. Troverai i dettagli qui sotto.

Riepilogo Ordine

- **Numero Ordine:** #56789
- **Data:** 6 Dicembre 2024
- **Metodo di pagamento:** Carta di credito
- **Totale:** €749,50

Indirizzo di Spedizione:

Via Roma 123
Milano, 20100

Articoli Ordinati:

- 1x Divano KIVIK 3 posti - **€399,00**
- 1x Tavolo BJURSTA allungabile - **€199,00**
- 4x Sedia ODGER - **€45,00/cad**

Stato dell'ordine:



Confermato



In transito

Per seguire la spedizione clicca qui:



Traccia il tuo ordine

Hai bisogno di aiuto?

Se hai domande sul tuo ordine, non esitare a contattarci:



support@ikea-servizi.com



Numero Verde IKEA: 800-123-456

Grazie per aver scelto IKEA. Non vediamo l'ora di aiutarti a rendere la tua casa più accogliente!

Il tuo team IKEA Italia 

Elementi Credibili

Struttura e Design:

L'email segue una struttura professionale e ordinata. Include elementi standard di una conferma d'ordine, come:

- Numero ordine (#56789).
- Totale spesa (€749,50).
- Articoli con prezzi plausibili (un divano, un tavolo e sedie).
- Indirizzo di spedizione, coerente con uno scenario di acquisto reale.

Linguaggio Professionale:

Il tono è formale, con frasi che rassicurano il cliente sullo stato dell'ordine. Inoltre, il messaggio non contiene errori grammaticali, una caratteristica che aumenta la fiducia.

Marchio Affidabile:

IKEA è un brand conosciuto e fidato. Utilizzare il nome di IKEA rende il phishing particolarmente efficace, poiché il destinatario potrebbe non sospettare un'email proveniente da un'azienda così nota.

Dettagli Specifici:

L'inclusione di articoli e costi rende l'email più autentica. Per esempio:

- Divano KIVIK 3 posti - €399,00.
- Tavolo BJURSTA allungabile - €199,00.
- 4x Sedia ODGER - €45,00/cad.

Questo tipo di personalizzazione può indurre la vittima a credere che l'ordine sia reale.

Elementi di Phishing

URL Malevolo:

Il link "Traccia il tuo ordine" rimanda a un dominio non ufficiale:

- Falso: <http://ikea-tracking-confirm.com>
- Ufficiale: gli URL IKEA reali seguono domini come <https://www.ikea.com/>.

Indirizzo Email sospetto:

L'indirizzo del mittente utilizza un dominio contraffatto:

- Falso: **support@ikea-servizi.com**.

- Ufficiale: IKEA utilizza indirizzi legati ai suoi domini principali, come **@ikea.com**.

Mancanza di Personalizzazione:

Sebbene l'email sembri autentica, non include il nome del destinatario (es. "Gentile Mario Rossi"). Le email reali di IKEA spesso personalizzano i messaggi per aumentare il livello di fiducia.

Pressione Indiretta:

Il link "Traccia il tuo ordine" potrebbe spingere la vittima a cliccare immediatamente, senza verificare la fonte, soprattutto perché l'acquisto è costoso (€749,50).

Perché l'Email Potrebbe Sembrare Credibile

Tematica Comune: Le email di conferma ordine sono normali per chiunque abbia acquistato online.

Dati Specifici e Realistici: Dettagli come prezzi, articoli e indirizzi fanno sembrare l'email autentica.

Assenza di Errori Evidenti: Molte email di phishing contengono errori grammaticali o traduzioni scadenti, ma questa email li evita.

Segnali di Allarme

Per evitare di cadere in trappola, ecco cosa verificare:

1. Controllare il dominio dell'email e del link: IKEA utilizza solo domini ufficiali.
2. Verificare la transazione: Se non hai effettuato acquisti, è probabile che l'email sia falsa.
3. Non cliccare su link sospetti: Passare il mouse sopra il link per vedere l'URL di destinazione prima di cliccare.
4. Contattare IKEA direttamente: In caso di dubbi, visitare il sito ufficiale e accedere al proprio account per controllare gli ordini.

Conclusione

Questa email di phishing dimostra come sia possibile imitare efficacemente comunicazioni reali per indurre le vittime a condividere dati sensibili. La sensibilizzazione su questi rischi e la verifica dei dettagli delle email sono essenziali per evitare frodi.