Consegna S5/L5

Scenario

La vittima in questo scenario è un professionista.
Durante l'anno, è comune per queste persone registrarsi a webinar, conferenze, o corsi di aggiornamento. Questo contesto offre un'opportunità perfetta per un attacco di phishing ben congegnato.

La vittima (Carla) riceve un'email che sembra provenire dal team organizzativo di una conferenza importante o di un evento legato alla propria carriera professionale. L'email contiene tutti gli elementi tipici di un'organizzazione legittima: un logo generico, toni formali e un URL che sembra autentico.

L'obiettivo del pishing qui è quello di raccogliere informazioni personali da rivendere o utilizzare in ulteriori attacchi (come il furto di identità o lo spear pishing), o magari ottenere accesso ad account specifici o eseguire transazioni faudolente.

E-mail

Oggetto: 📄 Conferma richiesta di partecipazione al corso Leadership 360° 2024

Corpo e-mail:
Gentile Carla,

Ti confermiamo che la tua iscrizione al corso intensivo Leadership 360° 2024, organizzato da Accademia Europea per il Management e la Crescita Personale, è stata ricevuta. Tuttavia, abbiamo riscontrato un problema tecnico che ha impedito il completamento della tua registrazione.

Per garantirti l’accesso al corso, ti chiediamo di confermare o aggiornare i dati della tua iscrizione entro le prossime 12 ore cliccando sul link sottostante:

👉 www.leadership-verifica.com

ATTENZIONE: Se non completi questa operazione entro il termine indicato, la tua prenotazione sarà cancellata e il tuo posto sarà riassegnato ad altri partecipanti.

Grazie per la tua collaborazione. Ci scusiamo per eventuali disagi e restiamo a tua disposizione per qualsiasi necessità.

Cordiali saluti,
Il Team Formazione
Accademia Europea per il Management e la Crescita Personale

Questo scenario funziona bene perché si basa su un contesto comune e familiare, ma con un tocco di urgenza e autorità. La vittima è meno propensa a verificare la legittimità dell'email poiché si sente "obbligata" a risolvere il problema velocemente.

Perchè è credibile:

In questo contesto, la vittima riceve un'email apparentemente professionale da un ente formativo credibile, come Accademia Europea per il Management e la Crescita Personale. L'email conferma una registrazione al corso Leadership 360° 2024, un nome che suona accattivante e reale. La vittima potrebbe aver effettivamente mostrato interesse per qualcosa di simile o, trovandosi coinvolta in molte attività, non ricordare con precisione se si è registrata davvero. Questo dubbio lavora a favore dell'attacco.
Il messaggio genera urgenza, dichiarando che c'è un problema tecnico nella registrazione e che i dati devono essere confermati entro 12 ore, altrimenti il posto verrà riassegnato. Questo tocco è fondamentale perché sfrutta il timore della vittima di perdere un'opportunità preziosa, spingendola ad agire in fretta senza riflettere troppo o controllare la legittimità dell'email.
Il link incluso (www.leadership-verifica.com) sembra autentico, ma conduce a un sito di phishing progettato per raccogliere informazioni personali, come dati di contatto, credenziali o persino dettagli di pagamento per presunte "quote di partecipazione".
Questo scenario funziona perché:

- È plausibile e non solleva sospetti immediati.
- Gioca sulla tendenza delle persone a fidarsi di enti educativi o formativi.
- Utilizza una scadenza imminente per indurre azioni impulsive.

Elementi sospetti

1. URL ingannevole

- Dettaglio sospetto: L'email include un link (www.leadership-verifica.com) che sembra legittimo, ma non è associato a un dominio ufficiale. Un ente formativo professionale userebbe il proprio dominio ufficiale (es. www.accademia-europea.com), mentre questo URL è generico e privo di autenticità.

2. Assenza di informazioni personali concrete

L'email non menziona informazioni specifiche dell'utente, utilizza solo il nome per mantenersi vaga. Un'email autentica avrebbe dettagli precisi per dimostrare la legittimità della comunicazione.

3. Urgenza non giustificata

L'email insiste sull'importanza di agire entro 12 ore per evitare la perdita del posto. Le comunicazioni ufficiali, infatti, di solito tendono a fornire più tempo per agire e non usano toni pressanti o minacciosi. L'urgenza è una tattica comune per indurre decisioni impulsive.

4. Errore tecnico non specificato

L'email afferma di aver riscontrato un problema tecnico, ma non specifica di che tipo di errore si tratti. Un ente professionale/formativo reale fornirebbe dettagli precisi per aiutare l'utente a risolvere il problema.

5. Mancanza di dettagli di contatto verificabili

L'email non offre un numero di telefono, un indirizzo fisico o altre modalità di contatto diretto per verificare la legittimità della comunicazione. Le organizzazioni affidabili forniscono sempre modi alternativi per mettersi in contatto.

Considerazioni finali

L'e-mail di pishing generata sfrutta diverse tecniche psicologiche e sociali per ingannare la vittima e convincerla ad agire senza pensarci troppo. Fa leva sull'urgenza e la paura di perdere un'opportunità e sulla manipolazione emotiva, nonchè sull'aspetto ufficiale avendo usato un nome generico per un corso di formazione, conferendo così all'e-email un aspetto autorevole.

Raccomandazioni

- Verificare l'email del mittente: prima di cliccare su qualsiasi link, è fondamentale esaminare l'indirizzo email del mittente. Un’email ufficiale proveniente da un ente riconosciuto avrà un dominio valido e pertinente (ad esempio @accademia-europea.com). Se l'indirizzo è generico o sospetto, come @gmail.com, è un segnale di allarme.
- Evitare di cliccare su link sospetti: non cliccare su link contenuti nelle email. Invece, accedere direttamente al sito web dell'ente formativo digitando l'URL nel browser, per evitare di essere reindirizzati a un sito di phishing.
- Non fornire mai informazioni sensibili via email: non inviare mai dati personali, numeri di carte di credito o altre informazioni sensibili rispondendo a una richiesta via email, specialmente quando non si è certi della legittimità del messaggio.
- Utilizzare l'autenticazione a due fattori (2FA): se possibile, abilitare sempre la verifica in due passaggi (2FA) per gli account online. Questo aggiunge una barriera in più contro gli accessi non autorizzati, anche se le credenziali sono state compromesse.
- Formazione e consapevolezza: è fondamentale educare gli utenti su come riconoscere e affrontare gli attacchi di phishing. La consapevolezza sui segnali di allarme aiuta a prevenire molti tentativi di inganno.