Hamine Khalil ashraf
Report Ingegneria sociale

1)descrizione dello scenario

- 1) Descrizione dello scenario

- Stiamo mandando un’email promozionale dall’agenzia un’agenzia di marketing chiamata “Evo Marketing Pro”, apparentemente professionale. L’oggetto è in occasione e urgente:

- La mail propone un pacchetto esclusivo per migliorare la visibilità del tuo brand online, disponibile solo per 24 ore. Contiene un link per accedere all’offerta e prenotare una consulenza gratuita.
- La mail è generica e firmata dal “Team di Evo Marketing Pro”.

Mittente:
promozioni@evo-marketingpro.co (dominio ingannevole che imita una vera agenzia)

Oggetto:

[OFFERTA LIMITATA] Aumenta la visibilità del tuo brand con il 70% di sconto!

Corpo dell'email:

Ciao!

Siamo felici di offrirti un pacchetto esclusivo per promuovee il tuo brand sui social media, disponibile solo per 24 ore.

Il nostro team di esperti ha già aiutato oltre 500 aziende a raddooppiare la loro visibilità online!

Clicca qui per accedere all'offerta e prenotare una consulenza gratuita:

www.evo-marketingpro.co/offerta-clienti

ATTENZIONE: l'offerta è valida fino alla mezzanotte di oggi.

A presto!
Il Team di Evo Marketing Pro

2) Perché potrebbe sembrare credibile

Ecco i motivi per cui potrebbe ingannare anche un utente attento:
1)Aspetto professionale: il layout dell'email è curato e il dominio (evo-marketingpro.co) sembra reale e coerente con il settore marketing.
2)Tono amichevole e convincente: usa un linguaggio diretto e informale, tipico delle comunicazioni aziendali moderne.
4)Richiamo all'autorità sociale: "abbiamo aiutato oltre 500 aziende" è una tecnica persuasiva basata sulla riprova sociale.
5)Offerta troppo vantaggiosa: uno sconto del 70% + consulenza gratuita crea l'illusione di un'occasione imperdibile.
5) è una classica mail di marketing promozionale di qualunque marchio aziendale

3)Analisi – Indicatori di phishing

1)Dominio ingannevole: evo-marketingpro.co sembra professionale, ma non è una fonte verificata.
2)Senso di urgenza: “solo per 24 ore” spinge all’azione impulsiva.
3)Link potenzialmente malevolo: anche se sembra una promozione, potrebbe portare a un sito fake per rubare dati.
4)Nessun riferimento specifico all’utente: email generica, tipica delle campagne di phishing.
5)Offerta troppo vantaggiosa: uno sconto del 70% + consulenza gratuita, poco credibile.