Ingegneria Sociali

S3 L5

Traccia

Esercizio di oggi: Siete stati chiamati da un'azienda di nome Epicodesecurity, questa azienda ha un sito web suo personale con il nome di dominio www.Epicodesecurity.it. un server email con l'email aziendale Epicodesecurity@semoforti.com

- Il vostro ruolo è quello di spiegare e informare i dipendenti dell'azienda Epicodesecurity sui rischi di attacchi di ingegneria sociale, in particolar modo contro il phishing.
- Come impostate la formazione? (spiegare cos'è il phishing).
- Cosa devono vedere, in particolar modo, i dipendenti per non cadere nel phishing?(quali parametri vedere per identificarlo.Esempio: SPF).

Il direttore vi da il permesso di creare un phishing controllato.

- Descrivere come agireste.(Usare dei programmi è opzionale).
- L'obiettivo è cercare di ingannare le persone nel miglior modo possibile.

Formazione

Cari dipendenti di Epicodesecurity,

Siamo lieti di informarvi che stiamo implementando un programma di formazione sulla sicurezza informatica per migliorare la consapevolezza dei rischi associati agli attacchi di ingegneria sociale, in particolare al phishing. La sicurezza delle informazioni è fondamentale per proteggere i nostri dati e garantire un ambiente di lavoro sicuro.

Cos’è l’ingegneria sociale?

L'ingegneria sociale è una forma di manipolazione psicologica in cui gli attaccanti cercano di sfruttare gli aspetti sociali e psicologici per raggiungere scopi malevoli, come l'accesso non autorizzato a informazioni riservate o sistemi informatici tutto attraverso l’inganno.

Cos’è il phishing?

Il phishing è una forma di attacco informatico in cui i malintenzionati cercano di ottenere informazioni sensibili, come nomi utente, password e dati finanziari, facendosi passare per entità affidabili, possono anche porre dei malware. Solitamente avviene attraverso e-mail, messaggi istantanei o siti web fraudolenti.

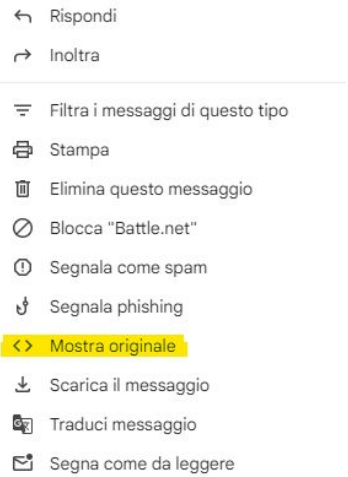
Obiettivi della formazione

Ogni giorno effettueremo 1 oretta come da programma una formazione allo scopo di raggiungere questi obiettivi.

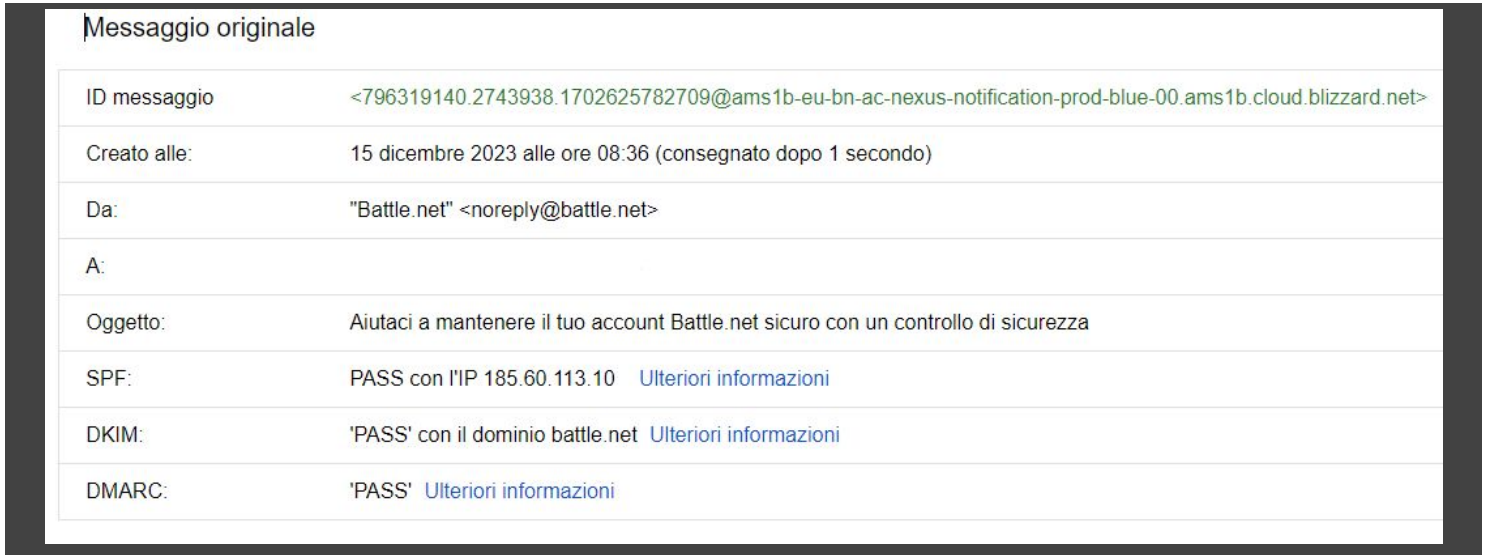
- Sensibilizzazione sull'importanza di verificare attentamente la provenienza delle comunicazioni e-mail.
- Identificazione di segnali di allarme nei messaggi, come richieste urgenti o minacce di conseguenze negative.
- Attenzione ai link sospetti e alle richieste di condividere informazioni personali.

Come verificare

Come prima cosa mettiamo caso che mi è arrivata una mail di phishing ed io la mia prima cosa che vado a fare è controllare grazie all'opzione “mostra originale”.



Come verificare



Messaggio originale

ID messaggio	<796319140.2743938.1702625782709@ams1b-eu-bn-ac-nexus-notification-prod-blue-00.ams1b.cloud.blizzard.net>
Creato alle:	15 dicembre 2023 alle ore 08:36 (consegnato dopo 1 secondo)
Da:	"Battle.net" <noreply@battle.net>
A:	
Oggetto:	Aiutaci a mantenere il tuo account Battle.net sicuro con un controllo di sicurezza
SPF:	PASS con l'IP 185.60.113.10 Ulteriori informazioni
DKIM:	'PASS' con il dominio battle.net Ulteriori informazioni
DMARC:	'PASS' Ulteriori informazioni

Come verificare

- Controlliamo l’**Indirizzo del Mittente**: Verificate sempre l'indirizzo e-mail del mittente per assicurarvi che provenga da una fonte attendibile.
- Controllare sempre **Link e Allegati**: Non cliccate su link o scaricate allegati da e-mail sospette o non richieste.
- L'implementazione di un **Autenticazione multi fattore** può aggiungere uno strato di sicurezza, anche se le credenziali vengono compromesse.
- Controlliamo **SPF, DKIM, DMARC**, vediamo a cosa servono.

Come verificare

SPF

Obiettivo: Verificare che l'indirizzo IP che invia un'email sia autorizzato a farlo per conto del dominio specificato.

Come funziona: Il proprietario del dominio specifica i server autorizzati nei record DNS SPF.

Come verificare

DKIM

Obiettivo: Garantire l'integrità e l'autenticità del contenuto di un'email mediante la firma digitale.

Come funziona: Il mittente firma il messaggio con una chiave privata, e il destinatario verifica la firma tramite la chiave pubblica nel record DKIM.

Come vericare

DMARC

Obiettivo: Fornire un meccanismo per l'autenticazione degli email e specificare come le email non autenticate dovrebbero essere gestite.

Come funziona: Unifica SPF e DKIM e aggiunge una politica di gestione dei messaggi non autenticati. Il proprietario del dominio dichiara una politica di gestione per i messaggi non autenticati e riceve report sulle attività tramite DMARC.

Phishing controllato

Il direttore mi ha dato l'autorizzazione di effettuare un Phishing controllato ai suoi dipendenti dopo la formazione, per controllare se i suoi dipendenti siano in grado di non farsi ingannare a questo tipo truffa. Ovviamente l'obiettivo essendo l'apprendimento non andrò ad intaccare le loro informazioni personali in alcun modo.

Il primo passo è creare una email realistica come la ricezione di dati, un aggiornamento di password, o un messaggio dal supporto IT, e devo far in modo che sia credibile con nomi simili e colori simili. Scelgo di creare una email di una banca (Unicredit) che mi chiede di aggiornare la password e di inserire le mie credenziali.

Phishing controllato

Buddibank <devlyna812@devlyn.com.mx>

buddy bank Powered by UniCredit

Ciao epicodesecurity abbiamo notato la tua richiesta di aggiornare la password.

Clicca qui

Questo è un esempio banale di quello che inviò ai dipendenti che ho formato e mettiamo caso che quasi tutti i dipendenti tranne due riescano a fare la procedura corretta, cioè verificare e dopodichè contattare la banca con il numero di telefono senza cliccare nella email. Gli altri due che hanno cliccato invece riceveranno un messaggio di avviso da parte mia che non hanno ben compreso i miei insegnamenti, (ovviamente non rubo nulla). Dopodichè vado a scrivere un report al direttore di com'è andata la situazione.