Progetto d’ Ingegneria Sociale

Traccia:

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 e-mail con l’e-mail aziendale Epicodesecurity@semoforti.com

1. 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.
2. Come impostate la formazione? (spiegare cos'è il phishing).
3. Cosa devono vedere, in particolar modo, i dipendenti per non cadere nel phishing? (quali parametri vedere per identificarlo. Esempio: SPF). Il direttore vi dà il permesso di creare un phishing controllato.
4. Descrivere come agireste. (Usare dei programmi è opzionale).
5. L'obiettivo è cercare di ingannare le persone nel miglior modo possibile.

2) Come impostare la formazione:

Se dovessi programmare una formazione per un’azienda per spigare cosa è il phishing farei un seminario della durata di una mattinata che andrebbe a spiegare cosa è il phishing e come evitarlo, preparerei una presentazione interattiva dividendo l’intera lezione in 5 moduli:

1. **Ruolo del Formatore:**

- Spiegare cosa sia il phishing e perché è una minaccia.
- Esempi di attacchi di phishing comuni e come possono apparire.
- L'importanza della consapevolezza e della formazione continua.

2. **Impostazione della Formazione:**

- Sessioni interattive che includono esempi pratici e simulazioni.
- Workshop dove i partecipanti possono analizzare e-mail sospette in un ambiente controllato.
- Discussione di casi di studio reali.

3. **Identificazione del Phishing:**

- Insegnare ai dipendenti a riconoscere i segnali di allarme come errori grammaticali, URL sospetti e mittenti non verificati.
- Spiegare come verificare l'autenticità delle e-mail (ad esempio, controllare gli header delle e-mail per autenticazione SPF/DKIM/DMARC).
- Utilizzo di strumenti di verifica e-mail per identificare tentativi di phishing.

4. **Creazione di un Phishing Controllato:**

- Ideare uno scenario di phishing che sia realistico ma chiaramente identificabile per scopi formativi.
- Invitare i dipendenti a individuare gli indizi che rivelano la natura fraudolenta dell'esercizio.
- Discutere le azioni corrette da intraprendere una volta identificato il tentativo di phishing.

5. **Obiettivi della Formazione:**

- Educare il personale su come riconoscere e reagire a tentativi di phishing.
- Migliorare la capacità dei dipendenti di proteggere informazioni sensibili.
- Creare una cultura della sicurezza all'interno dell'organizzazione dove la prevenzione del phishing è una priorità.

3) Cosa devono vedere, in particolar modo, i dipendenti per non cadere nel phishing?

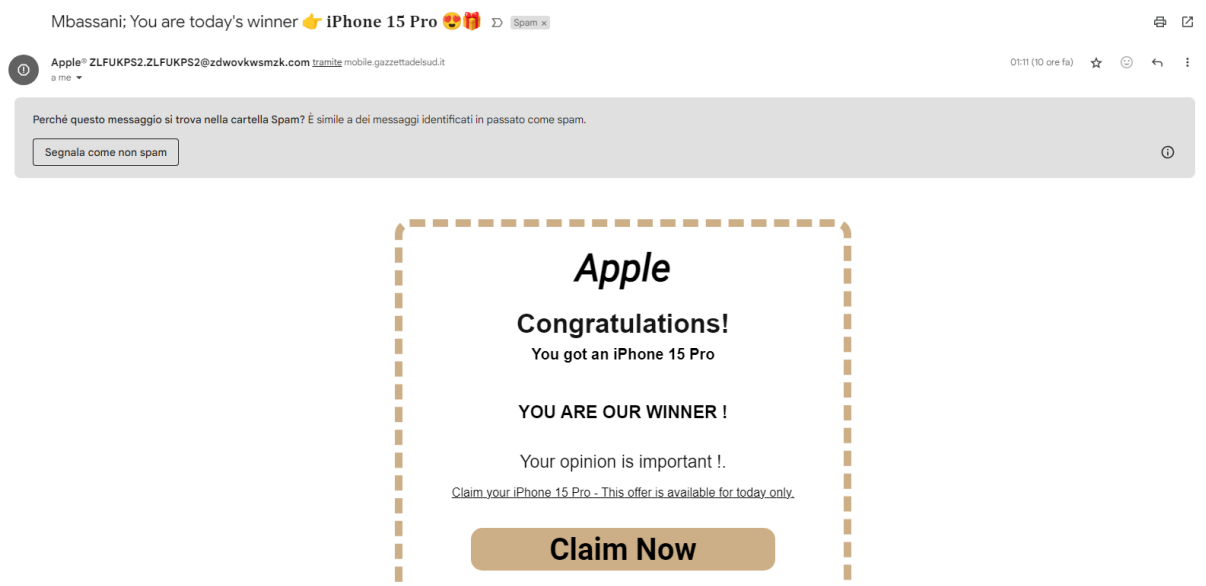
I dipendenti devono far particolarmente attenzione a errori grammaticali nel nome del mittente o del sito web di destinazione, URL sospetti e mittenti non verificati all'autenticità dell'e-mail controllando gli header SPF/DKIM/DMARC (come qui sotto in esempio) tramite l'impostazione mostra originale dell'e-mail che si sta visualizzando.

ID messaggio	<CAK7sKKm0WjyrCs5JyDb2GOV9DZnWbYUX2TfF28okZ_=wjsUj1A@mail.gmail.com>
Creato alle:	5 dicembre 2023 alle ore 20:21 (consegnato dopo 12 secondi)
Da:	Finanziamenti EPICODE <finanziamenti@epicode.com>
A:	Finanziamenti EPICODE <finanziamenti@epicode.com>
Oggetto:	comunicazione importante finanziamento "per Merito"
SPF:	PASS con l'IP 209.85.220.41 Ulteriori informazioni
DKIM:	'PASS' con il dominio epicode.com Ulteriori informazioni
DMARC:	'PASS' Ulteriori informazioni

Se tutti e tre gli header presentano lo stato di PASS vuol dire che l'e-mail è partita dal server e-mail originale di tale azienda e il mittente è verificato ma questo a volte non ne garantisce la sicurezza al 100% perché se l'attaccante è già dentro i sistemi di quell'azienda tutte le e-mail che invia sono automaticamente verificate.

E-mail di phishing tipica esempio:

In questa e-mail di esempio si può notare come l'inizio del nome del mittente sia Apple e poi contiene lettere e numeri a caso, e se si va a vedere il link allegato al tasto claim now senza cliccarlo si capisce subito che non porta direttamente al sito di Apple ma molto probabilmente ad un sito fake che avrà lo scopo di farvi scaricare un malware rendendo il vostro computer compromesso senza che ve ne accorgiate.



Messaggio originale

ID messaggio	<zl79du69.zl79du69.zl79du69.javamail.tomcat@pdr8-services-05v.prod.zl79du69
Creato alle:	15 dicembre 2023 alle ore 01:11 (consegnato dopo 1 secondo)
Da:	Apple® <ZLFUKPS2.ZLFUKPS2@zdwovkwsmzk.com>
A:	m.bassani97@gmail.com
Oggetto:	Mbassani; You are today's winner 👉 iPhone 15 Pro 😍🎁
SPF:	PASS con l'IP 82.223.12.140 Ulteriori informazioni

Se il dipendente è ancora dubbioso sull'autenticità dell'e-mail perché l'attaccante ha clonato l'e-mail tutto e per tutto da una fonte ufficiale che il dipendente conosce, ma l'indirizzo e-mail del mittente e totalmente diverso dal solito, il dipendente può andare a vedere l'autenticità di uno o più degli header dell'e-mail, e se questi risultano mancanti come per esempio in questa e-mail di phishing dove il DKIM/DMARC mancano il dipendente dovrebbe riportare il fatto al servizio IT dell'azienda e chiedere delucidazioni su tale email.

Successivamente allo svolgimento del seminario in azienda con i dipendenti ci si può mettere d'accordo con il direttore per fare una prova di phishing controllato da svolgere entro 30-45 giorni dalla data del seminario per vedere se i dipendenti hanno capito le nozioni di base per evitare le e-mail di phishing. Da notare che bisogna avvertire il direttore che se alcuni dei suoi dipendenti cadono vittima del phishing controllato potrebbero sentirsi emotivamente traditi e potrebbero intentare una querela contro l'azienda.

4/5) Descrivere come agireste per lo svolgimento del phishing controllato e come inganneresti i dipendenti.

Se fossi responsabile per lo svolgimento del phishing controllato andrei a comprare un dominio simile a www.Epicodesecurity.it per esempio www.Epicdesecuriti.it dove sostituisco la y con la i.

Successivamente andrei ad usare il tool Set di Kali Linux per clonare il sito ufficiale dell'azienda nello specifico la pagina di login per i dipendenti o una pagina dell'azienda che vada a richiedere delle credenziali di accesso. Collegherei la pagina clonata al nostro dominio fasullo in modo tale da essere più difficile da riconoscere dai dipendenti. Dopodiché andrei creare un indirizzo e-mail simile a quello aziendale Epicodesecurity@semoforti.com per esempio Epicodesecurity@semopiùforti.com la collegherei ad un server proxy per mostrare la credibilità del mio indirizzo IP e scriverei un'e-mail contenenti i formati e i design dell'azienda per esempio:

e-mail mittente: Epicodesecurity@semopiùforti.com

Oggetto: Importante Avviso di Sicurezza - Azione Richiesta

Cari dipendenti,

Ci rivolgiamo a voi dal Dipartimento di Sicurezza Aziendale per informarvi di una situazione importante che richiede la vostra immediata attenzione.

Nel corso della giornata odierna, il nostro sistema di login aziendale ha riscontrato un problema tecnico che potrebbe comportare la perdita dei progressi di lavoro fatti durante la giornata. Per evitare questa situazione spiacevole e garantire la sicurezza delle vostre informazioni e dei vostri progetti, vi chiediamo di eseguire una seconda procedura di login urgente al seguente link:

www.Epicdesecuriti.it

Vi preghiamo di procedere con il login al più presto possibile per evitare perdite di dati e progressi di lavoro. Il link fornito vi condurrà a una pagina sicura dove potrete effettuare il login come al solito. Una volta effettuato il login, potrete tornare a lavorare ai vostri progetti senza alcuna perdita di dati.

Ricorda che questa azione è essenziale per garantire la continuità del vostro lavoro e proteggere le vostre informazioni personali e aziendali. Il Dipartimento di Sicurezza Aziendale sta monitorando attentamente la situazione e sta lavorando per risolvere il problema tecnico quanto prima.

In caso di difficoltà o domande relative a questa procedura di login, vi preghiamo di contattare il nostro servizio di assistenza tecnica al seguente indirizzo e-mail o numero di telefono:

Epicodesecurity@semopiùforti.com

+39 3333333333

Ti ringraziamo per la vostra collaborazione e comprensione in questa situazione. La vostra sicurezza e la vostra continuità del lavoro sono la nostra massima priorità.

Cordiali saluti,

Dipartimento di Sicurezza Aziendale

Epicode