

Gestione delle e-mail sospette

Imparare a gestire le e-mail sospette è essenziale per mantenere la propria azienda difesa dai criminali informatici. Se non gestisci correttamente un'e-mail sospetta, potresti cadere vittima di un attacco di phishing.

Segui i suggerimenti in basso per avere la certezza di gestire correttamente le e-mail sospette:

Non rispondere all'e-mail

Se ricevi un'e-mail sospetta che sembra provenire da qualcuno che conosci, potresti essere tentato di rispondere all'e-mail per avere ulteriori informazioni. Tuttavia, se rispondi all'e-mail, potresti andare incontro a un rischio per la sicurezza. Se un account e-mail è stato compromesso, la persona che ti risponde probabilmente non sarà quella che credi. In realtà potresti comunicare con un criminale informatico.

Non inoltrare l'e-mail

La pratica migliore è quella di non fare mai clic su un link e non aprire un allegato che non stavi aspettando. Tuttavia, se sei stato ingannato da un'e-mail di phishing e hai fatto clic su un link dannoso o hai aperto un allegato dannoso, potresti scoprire che il link o l'allegato non si comporta come previsto. Ad esempio, se apri un allegato con un'immagine sospetta, il file potrebbe in realtà aprire una finestra di installazione. Oppure, se fai clic su un link dannoso, il link potrebbe reindirizzarti a una falsa pagina di accesso.

Se il link o l'allegato è sospetto, potresti essere tentato di inoltrare l'e-mail a qualche collega per chiedere aiuto. Tuttavia, inoltrare l'e-mail a un collega potrebbe aumentare il rischio. Se fai clic su un link o apri un allegato, considera qualsiasi comportamento insolito come un campanello d'allarme. Non inoltrare mai e-mail insolite o sospette ad altri utenti. Se inoltri un'e-mail di phishing, aumenti il rischio di incorrere in una violazione della sicurezza perché anche il tuo collega potrebbe fare clic sul link di phishing.

Non contrassegnare l'e-mail come spam

Le e-mail di spam sono solitamente pubblicità indesiderate. Sebbene le e-mail di spam siano spesso fastidiose, solitamente sono innocue. Tuttavia, un attacco phishing è un'e-mail dannosa progettata per sembrare un messaggio legittimo. Le e-mail di phishing generalmente richiedono di compiere un'azione, come fare clic su un link, aprire un allegato o anche trasferire del denaro.

Se contrassegni un'e-mail sospetta come spam, l'e-mail verrà spostata in un'altra cartella insieme a tutte le altre e-mail dello stesso mittente. Quindi, se sposti l'e-mail sospetta in una cartella di spam, l'e-mail verrà nascosta. Tuttavia, il problema non sarà risolto.

Suggerimenti per mantenere la sicurezza

Il modo migliore per gestire un'e-mail sospetta è quello di segnalarla alla tua azienda. Se segnali l'e-mail, il tuo team IT potrà valutare e mitigare la minaccia.

Quando ricevi un'e-mail sospetta, per mantenere la sicurezza segui questi consigli:

- Assicurati di seguire la procedura stabilita dalla tua azienda per la segnalazione delle e-mail sospette. Seguire i protocolli di sicurezza informatica aiuterà a mantenere i dati di tutti al sicuro.
- Se non sai come segnalare l'e-mail, lascia l'e-mail nella tua casella di posta e chiedi aiuto a un manager o a un supervisore.
- Se non sei sicuro se un'e-mail è spam o un attacco di phishing, segnala l'e-mail e il tuo team IT gestirà la situazione.



Il team di sicurezza KnowBe4