

Cómo lidiar con correos electrónicos sospechosos

Saber lidiar con correos electrónicos sospechosos es esencial para proteger su organización contra los ciberdelincuentes. Si no lo hace correctamente, podría convertirse en la víctima de un ataque de phishing.

Siga estos consejos para gestionar correctamente los correos electrónicos sospechosos:

No responda al correo

Si recibe un correo electrónico sospechoso y el remitente le resulta familiar, es posible que tenga la tentación de responder para obtener más información. Sin embargo, su respuesta podría aumentar el riesgo de seguridad. Si una cuenta de correo electrónico se ha visto comprometida, probablemente la persona que le responda no sea quien espera. En realidad, podría estar hablando con un ciberdelincuente.

No reenvíe el correo

La práctica recomendada es no hacer nunca clic en un enlace ni abrir un archivo adjunto que no esperaba recibir. No obstante, si cae en el engaño de un correo electrónico de phishing y hace clic en un enlace malintencionado o abre un archivo adjunto malicioso, es posible que estos no tengan el comportamiento esperado. Por ejemplo, si abre una imagen adjunta sospechosa, el archivo podría abrir una ventana de instalación. O, si hace clic en un enlace malintencionado, este podría redirigirle a una página de inicio de sesión falsa.

Si sospecha de un enlace o archivo adjunto, quizá piense en reenviarlo a un compañero de trabajo para que le ayude. No obstante, esto podría aumentar el riesgo. Si hace clic en un enlace o abre un archivo adjunto, considere cualquier comportamiento inusual como una señal de alarma. Nunca reenvíe correos electrónicos inusuales o sospechosos a otros usuarios. Si reenvía un correo electrónico de phishing, aumenta el riesgo de que se produzca una violación de seguridad, ya que su compañero de trabajo también podría hacer clic en el enlace de phishing.

No marque un correo como spam

Los correos electrónicos que reconocemos como spam suelen ser publicidad no deseada. Si bien pueden ser molestos, suelen ser inofensivos. Sin embargo, un ataque de phishing es un correo electrónico malicioso diseñado de modo que parezca un mensaje legítimo. Los correos electrónicos de phishing suelen incluir una llamada a la acción, como hacer clic en un enlace, abrir un archivo adjunto o incluso transferir dinero.

Si marca como spam un correo electrónico sospechoso, lo moverá a otra carpeta junto con el resto de los correos electrónicos del mismo remitente. Por lo tanto, si traslada el correo electrónico sospechoso a una carpeta de spam, quedará oculto. Pero no se habrá resuelto el problema.

Consejos para protegerse

La mejor forma de lidiar con un correo electrónico sospechoso es denunciándolo a su organización. Si lo denuncia, el equipo de TI puede evaluar y mitigar la amenaza.

Cuando reciba un correo electrónico sospechoso, siga estos consejos para protegerse:

- Asegúrese de seguir el proceso de su organización para denunciar correos electrónicos sospechosos. Si sigue los protocolos de ciberseguridad, ayudará a proteger la información de todo el mundo.
- Si no sabe cómo denunciar el correo, déjelo en su bandeja de entrada y recurra a un gerente o supervisor.
- Si no sabe con certeza si un correo electrónico es spam o un ataque de phishing, denúncielo y el equipo de TI se encargará.



El equipo de seguridad de KnowBe4