

Cómo tratar correos electrónicos sospechosos

Aprender a tratar correos electrónicos sospechosos es crucial para mantener la seguridad de la organización en la que trabaja frente a ciberdelincuentes. Si no se realiza un correcto tratamiento de un correo electrónico sospechoso, podría ser víctima de un ataque de phishing.

Siga estos consejos para asegurarse de que trata los correos electrónicos de forma correcta:

No responda el correo electrónico

Si recibe un correo electrónico sospechoso que parece provenir de una persona que conoce, es posible que le tiente responder el correo electrónico para obtener más información. Sin embargo, si responde, podría haber un mayor riesgo de seguridad. Si una cuenta de correo electrónico queda expuesta, es posible que la persona que le responda no sea quien usted espera. De hecho, podría estar comunicándose con un ciberdelincuente.

No reenvíe el correo electrónico

La práctica recomendada consiste en nunca hacer clic en un enlace para abrir un archivo adjunto que no estaba esperando. Si cae en la trampa de un correo electrónico de phishing y hace clic en un enlace malicioso o abre un archivo adjunto malintencionado, es posible que descubra que el enlace o el archivo adjunto no eran lo que esperaba. Por ejemplo, si abre un archivo adjunto de imagen sospechoso, el archivo en realidad podría abrir una ventana de instalación. Por otro lado, si hace clic en un enlace malicioso, es posible que este redirija a una página falsa de inicio de sesión.

Si el enlace o el archivo adjunto son sospechosos, quizá considere reenviar el correo electrónico a un colega para solicitar su ayuda. No obstante, reenviar el correo electrónico a un colega podría aumentar el riesgo. Si hace clic en un enlace o abre un archivo adjunto, considere que cualquier comportamiento inusual es 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 una violación de seguridad porque su colega también podría hacer clic en el enlace de phishing.

No marque el correo electrónico como correo no deseado (spam)

Los correos no deseados suelen ser anuncios que no pretende recibir. A pesar de que los correos no deseados pueden ser molestos, suelen ser inofensivos. Sin embargo, un ataque de phishing se realiza con un correo electrónico malicioso diseñado para que luzca como un mensaje real. En general, los correos electrónicos de phishing incluyen una llamada a la acción, como hacer clic en un enlace, abrir un archivo adjunto o incluso transferir dinero.

Si marca un correo sospechoso como correo no deseado, este se moverá a una carpeta diferente junto a todos los demás correos electrónicos del mismo remitente. Por lo tanto, si mueve el correo sospechoso a la carpeta Correo no deseado, se ocultará el correo electrónico. Pero el problema no se resolverá.

Consejos para conservar la seguridad

La mejor manera de tratar un correo electrónico sospechoso es reportarlo a la organización. Si reporta el correo electrónico, el equipo de TI podrá evaluarlo y reducir la amenaza.

Siga los siguientes consejos cuando reciba un correo electrónico sospechoso para mantener la seguridad:

- Asegúrese de seguir el proceso de la organización en la que trabaja para reportar correos electrónicos sospechosos. Si acata los protocolos de ciberseguridad, se podrá mantener a salvo la información de todas las personas.
- Si no sabe cómo reportar el correo electrónico, deje el correo en la Bandeja de entrada y consulte con el gerente o supervisor para obtener ayuda.
- Si no tiene la seguridad de si un correo electrónico es un correo no deseado o un ataque de phishing, repórtelo y el equipo de TI se encargará de la situación.

