22 de junio 2022

CYBERSECURITY AWARENESS

SEGURIDAD

¿Cómo identificar correos electrónicos sospechosos Phishing, Spear Phishing y Spam?

¿Correo electrónico de Phishing?

El phishing es el proceso de intentar adquirir información sensible como: nombres de usuario, contraseñas o detalles financieros, haciéndose pasar por una entidad de confianza mediante el uso de correo electrónico masivo que intenta evadir los filtros de spam.

Características:

- Remitente desconocido.
- Intención de apelar a las emociones.
- Solicitud para hacer clic en un enlace o descargar un archivo.
- Parece provenir de una organización que brinda confianza.

¿Correos electrónicos de Spear Phishing?

Spear Phishing, es un correo electrónico dirigido a un individuo o departamento específico dentro de una organización que parece provenir de una fuente de confianza. En realidad son ciberdelincuentes que intentan robar información confidencial.

Características:

- Remitente desconocido.
- Intención de apelar a las emociones.
- Sentido de urgencia.
- Solicitud para hacer clic en un enlace o descargar un archivo.
- En ocasiones parece provenir de una organización de confianza.

¿Correo electrónico Spam?

El correo electrónico spam, también conocido como correo basura, se refiere a mensajes no solicitados enviados en masa con el propósito de anunciar un producto o servicio.

Report Phishing

¿Cómo reportar un correo electrónico sospechoso?

Si recibes un correo electrónico sospechoso, puedes denunciarlo utilizando el botón de denuncia de Cofense que se encuentra en la barra de herramientas de Microsoft Outlook, medio que reenviará el correo al Equipo Global de Seguridad de la información (GIS) a la casilla **gis@brinksinc.com**

Jorge Briones

Director de Tecnología, Nuevos Negocios y Proyectos Estratégicos

BRINKS