Campus Seguro UAO

¡Aprendamos juntos sobre seguridad informática y evitemos fraudes!

¿Cómo reconocer un evento de ‘phishing’?

Recuerda que las empresas o entidades nunca solicitan información confidencial por correo electrónico, mensajes de texto, mensajes de WhatsApp o redes sociales; ellos tienen protocolos de seguridad para la actualización de datos a través de sus medios oficiales.

Aunque la dirección del remitente puede ser manipulada por el estafador, se presentan delincuentes que dejan al descubierto éste dato, observa si la dirección del remitente es sospechosa.

Es sospechoso si llegan correos electrónicos de entidades o empresas con las cuales no tienes relación o nunca has asociado el buzón de correo donde te llegó el mensaje.

No creas todo lo que dicen, los mensajes fraudulentos tienen el objetivo de desinformar, engañarnos o infectarnos para sacar provecho.

¿Cómo protegerse de ser víctima de ‘phishing’?

No respondas ni abras ningún enlace que esté asociado en los mensajes sospechosos. Si deseas consultar, hazlo directamente escribiendo la URL oficial de la entidad o empresa en el explorador o llama a la entidad para verificar los hechos.

Vence la curiosidad y no descargues archivos adjuntos que estén contenidos en éste tipo de correos, podría contener software malicioso.

Cuando requieras introducir información confidencial en una web, estas son consideradas seguras si su dirección contiene una ‘s’ después del http (https://...) y se visualiza un candado cerrado a su lado izquierdo.

Si sospechas que fuiste víctima de ‘phishing’, cambia inmediatamente tus contraseñas y contacta a la entidad para reportar lo sucedido.

Reporta tus sospechas al correo nchicaiza@uao.edu.co de la Dirección de Tecnologías de Información.