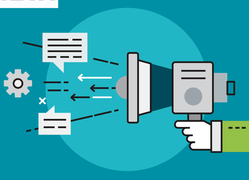
semsin

TIPS para no ser víctima de la falsificación



CÓMO DETECTAR CORREOS FALSOS

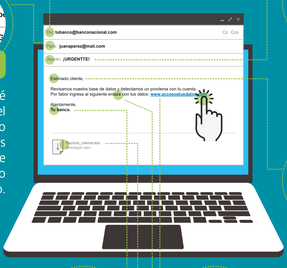
Los correos de phishing y los que esconden adjuntos maliciosos buscan llamar la atención de sus víctimas y lograr que proporcionen sus credenciales o se infecten. Pero, si miras con cuidado, encontrarás las señales que indican que es un engaño.

Remitente

Desconocido, aunque puede usar un dominio que luzca normal como "@bancanacional.com". Pero ¿eres su cliente o jamás habías tratado con esa entidad?

Destinatario

Puede que solo esté tu email, que el campo esté vacío o figuren otras direcciones, que implican un envío masivo.



Asunto

Urgencia, pedido de que pagues, revises o actualices una cuenta o servicio.

Encabezado

Se dirige a un usuario genérico.

Firma

Imita a un banco o cualquier compañía conocida que inspire confianza. Se copian el logo y la estética, y quizá hasta nombres de sus representantes.

Enlace

Fíjate a dónde dirige, ya sea que esté acortado o no. Las URL pueden acortarse o falsificarse para esconder el verdadero destino.

Adjunto

El ransomware y otras formas de malware siguen usando archivos infectados para propagarse.

Mensaje

Faltas de ortografía, mala redacción, amenaza de que algo grave ocurrirá si no haces lo que te piden.

CONSEJO

6 CLAVES PARA RECONOCER CORREOS DE PHISHING

CÓMO DETECTAR SITIOS FALSOS

Si bien algunos sitios web falsos son réplicas casi idénticas de los originales, hay patrones similares para detectarlos:

HTTPS:

¿Usa un protocolo seguro?

URL

¿Es la misma que recuerdas o que figura en Google para esa entidad? Presta atención a alteraciones difíciles de percibir como bannconacional.com

Estructura

¿Funciona y luce como el sitio de una entidad, con encabezados y menús desplegables, o solo hay un formulario sin nada alrededor?

Formulario

¿Te pide más datos de lo habitual? Si ingresas una contraseña errónea, ¿lo advierte o la toma como válida?

CONSEJO

CÓMO SE ESCONDE EL PHISHING EN URL FALSAS

Las señales funcionan en conjunto y puede que un correo con encabezado impersonal sea legítimo, o que la compañía cometa un error ortográfico en su comunicado, o que su sitio todavía no tenga un certificado de seguridad. Por eso, debes prestar atención a varias cosas a la vez para detectar un engaño.

¿CUÁNTO PODRÍA LLEGAR A GANAR UN CIBERCRIMINAL?

Cuando un cibercriminal obtiene las credenciales válidas (usuario+contraseña) de un usuario, puede venderlas en la Dark Web por alrededor de dos dólares.

Un phishing que alcance 18.000 clics. Suponiendo que ⅓ de los usuarios ingresaron sus credenciales de Facebook...

18.000 personas hicieron clic

9.000 ingresaron sus credenciales de Facebook

2 € por cuenta

18.000 € de ganancia