IDENTIFIQUEMOS UN PHISHING

Colnodo
Uso estratégico de
Internet para el desarrollo

ESCUELA DE SEGURIDAD DIGITAL

www.escueladeseguridaddigital.co

PHISHING

¡URGENTE! han hackeado tu cuenta bancaría 2

No reply - usuario <nohackconfio@tehackeo.com> 1

para mí

¡URGENTE! han hackeado tu cuenta bancaría 3

Estimado usuario de Banco Z

Le notificamos que hemos detectado un ingreso sin autorización a nuestos canales de atención. Le solicitamos acomedidamente que ingrese a nuestra página web para cambiar su contraseña. 4

Atención usuarios banco Y

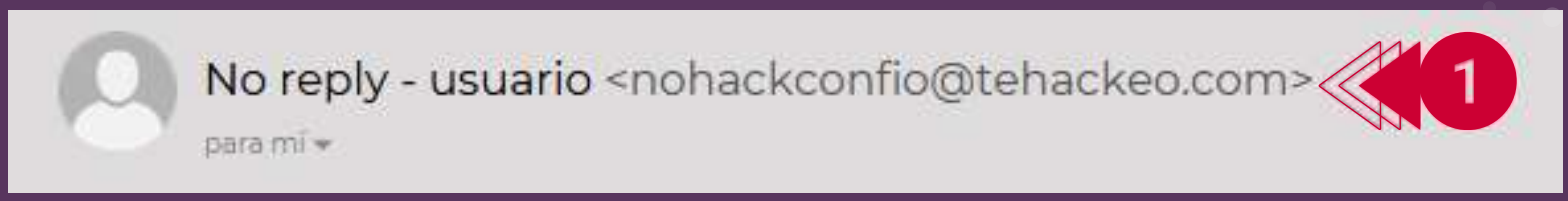
Gracias por contar siempre con nosotros
Un cordial saludo.
Banco Z

AWS reInvent _ 2... 6

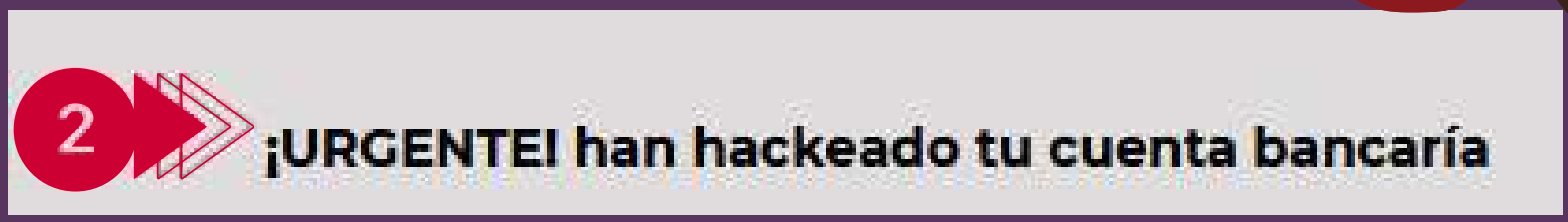
http://soyunenlacequetequiererobartuinformacion.lt.co/no-confies/lee-muy-bien-cada-enlace 5

ESCUELA DE SEGURIDAD DIGITAL

1 ¿Esperabas este email?
Comprueba que el email coincida con la persona o entidad **remitente** que dice ser o si está suplantando a alguien.



2 ¿Capta tu atención el **asunto** del correo?
La mayoría de correos fraudulentos utilizan **asuntos llamativos** e impactantes para captar tu atención. Entre la premura no nos fijamos en los pequeños detalles que nos ayudarán a identificar el phishing.



3 ¿Cuál es el **objetivo** del correo?
Una entidad de servicios como el banco u otros, **nunca te pedirán tus datos personales por correo**. Además, si es de carácter urgente, amenazante o con ofertas y promociones muy atractivas, es muy posible que sea un **fraude**.

¡URGENTE! han hackeado tu cuenta bancaría 3

4 ¿Tiene **errores ortográficos** o parece una mala traducción de otro idioma?
Revisa la redacción en busca de **errores de ortografía** o gramaticales.

Estimado usuario de Banco Z

Le notificamos que hemos detectado un ingreso sin autorización a nuestos canales de atención. Le solicitamos acomedidamente que ingrese a nuestra página web para cambiar su contraseña. 4

Atención usuarios banco Y

Gracias por contar siempre con nosotros
Un cordial saludo.
Banco Z

5 ¿Los **enlaces** lo llevan a una página legítima? Sitúa el cursor encima del **enlace**, o mantén presionado el enlace en dispositivos móviles, podrás ver la **URL** real a la que redirige. Si no coincide o es una web sin certificado de seguridad **(https://)**, NO debes hacer clic.

6 ¿Contiene un **archivo adjunto** sospechoso? Analiza los **adjuntos** antes de abrirlos, puede tratarse de un malware. Los antivirus y analizadores de ficheros te ayudarán a identificar si están infectados.

Colnodo

Uso estratégico de
Internet para el desarrollo

ESCUELA DE SEGURIDAD DIGITAL

WWW.ESCUELADESEGURIDADDIGITAL.CO
WWW.COLNODO.APC.ORG

@COLNODO