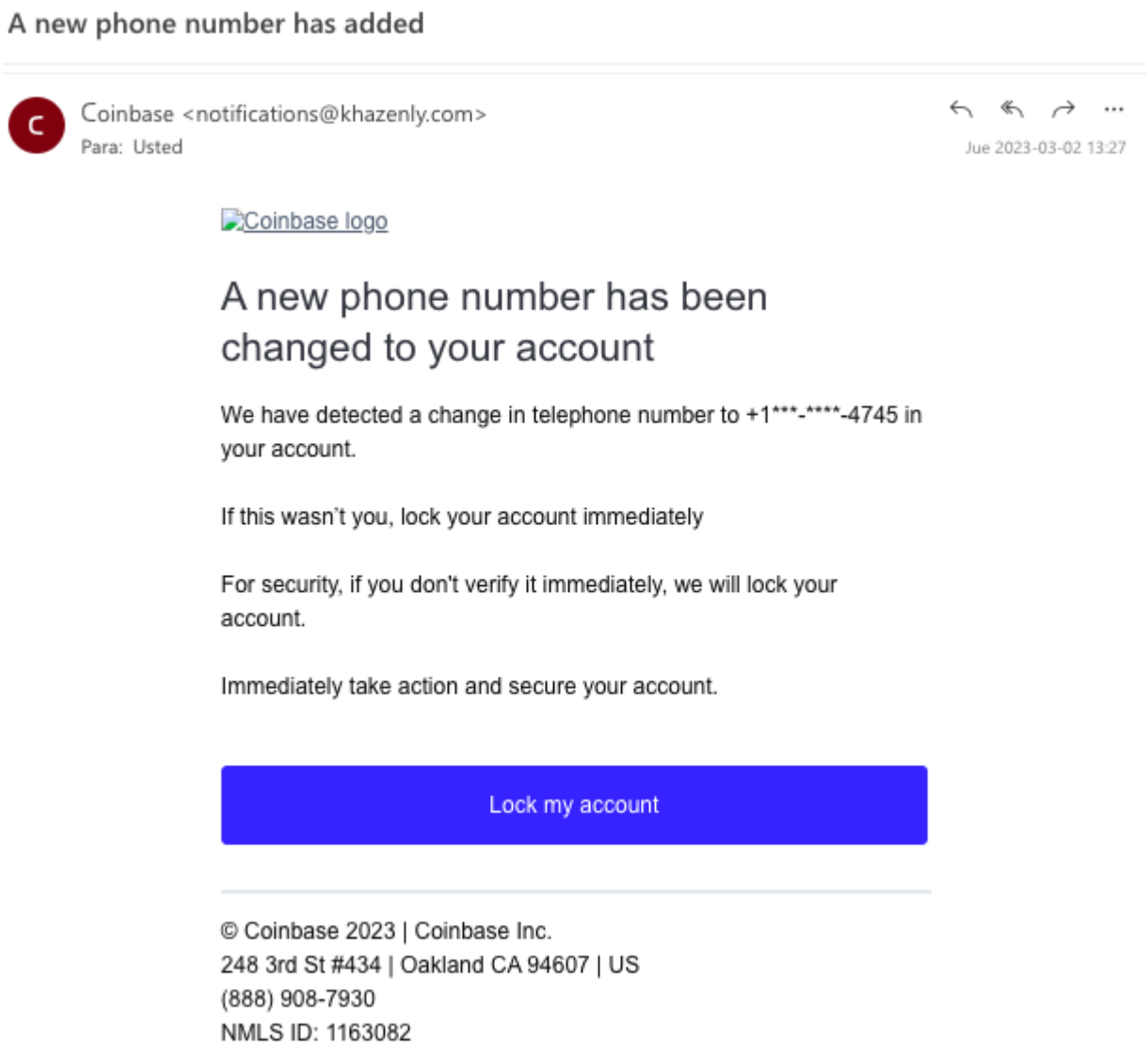
Coinbase (web spoofing y phishing)



A new phone number has added

Coinbase <notifications@khazenly.com>
Para: Usted
Jue 2023-03-02 13:27

Coinbase logo

A new phone number has been changed to your account

We have detected a change in telephone number to +1***-****-4745 in your account.

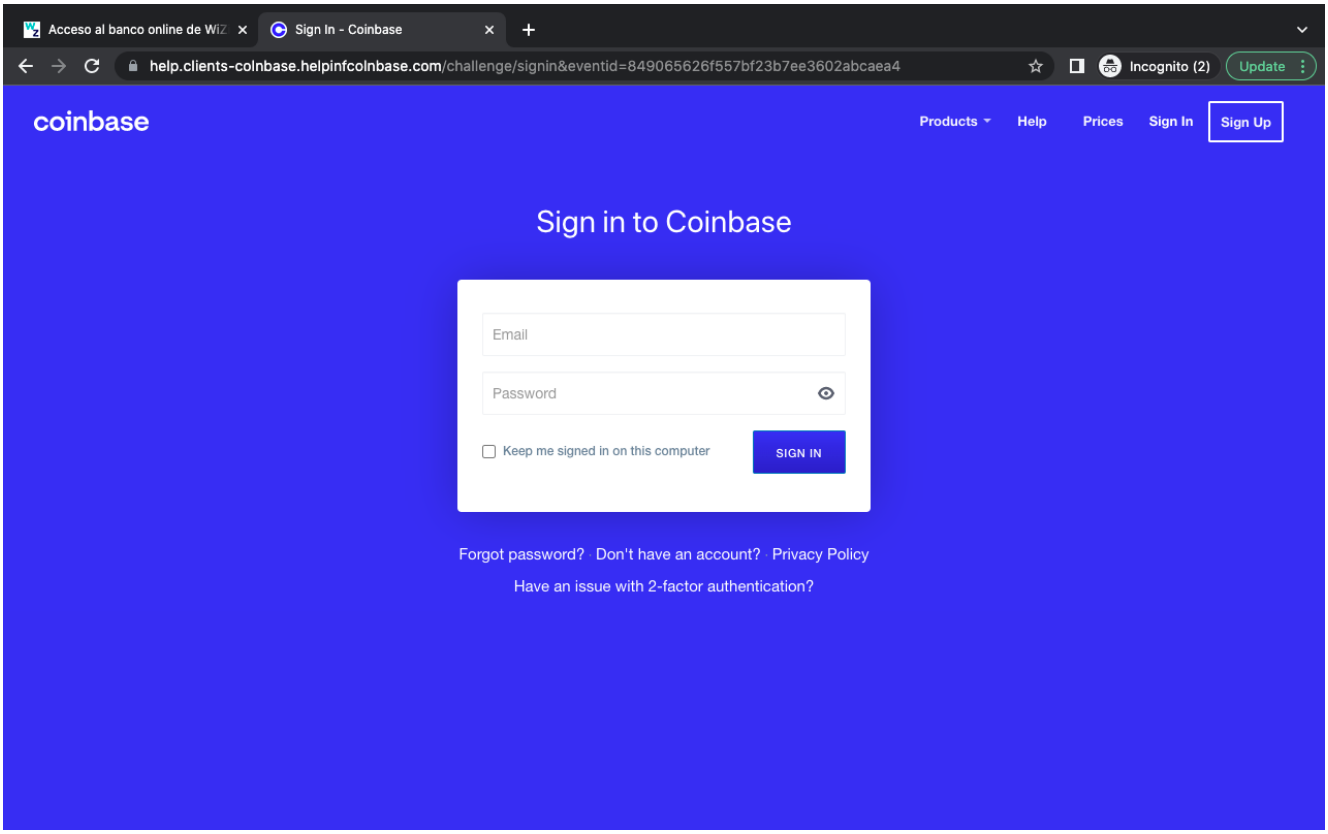
If this wasn't you, lock your account immediately

For security, if you don't verify it immediately, we will lock your account.

Immediately take action and secure your account.

Lock my account

© Coinbase 2023 | Coinbase Inc.
248 3rd St #434 | Oakland CA 94607 | US
(888) 908-7930
NMLS ID: 1163082



Web Spoofing y phishing son dos tipos de ataques cibernéticos que tienen como objetivo engañar a los usuarios para que proporcionen información confidencial, como contraseñas o datos financieros. Aunque ambos tipos de ataques son similares en su objetivo final, existen algunas diferencias importantes entre ellos.

Web Spoofing es un tipo de ataque en el que los atacantes crean una página web falsa que imita una página web legítima. El objetivo de la página falsa es engañar al usuario para que introduzca su información de inicio de sesión o información financiera, creyendo que está en una página web legítima. Este tipo de ataque se logra mediante el uso de técnicas de ingeniería social, como el envío de correos electrónicos fraudulentos que dirigen al usuario a la página falsa.

Por otro lado, el phishing es un tipo de ataque en el que los atacantes envían correos electrónicos fraudulentos o mensajes de texto que parecen provenir de una fuente legítima, como un banco o una empresa conocida. El objetivo del correo electrónico o mensaje de texto es engañar al usuario para que

haga clic en un enlace malicioso que dirige al usuario a una página web falsa donde se le solicita su información de inicio de sesión o información financiera.

En resumen, la principal diferencia entre Web Spoofing y phishing es que Web Spoofing implica la creación de una página web falsa, mientras que phishing implica la creación de un correo electrónico o mensaje de texto falso. Sin embargo, ambos tipos de ataques utilizan técnicas de ingeniería social para engañar al usuario y obtener información confidencial.