

Date: Wed, 1 May 2024 20:04:16 +0000

Subject: Your Bank Account has been blocked due to unusual activities

To: bob.sanders@corhalitech.com

From: alerts@chase.com

Return-Path: kellyellin426@proton.me

Sender IP: 185.70.40.140

Resolve Host: 185-70-40-140.protonmail.ch

Message-ID: <i7g9MMh5NtErta0zQZEp3D-i-u3FWwdo0wY5mhD8Q1vIvv1yeLj-jMWPAn-HP3FugKsucsWSub00Vns8GRFYG0aH4MyU2paqP6yUnRcgaU=@protonmail.com>

URL:

<https://dsgo.to/CQECQECnpqY3NDSGtODt9ft2qtxzcXGUveTV5fRYmtYAZsQCnpqY3NDSGtODt9ft2qtxzcXGUveTV5fRYmtYAZsQCQECnpqY3NDSGtODt9ft2qtxzcXGUveTV5fRYmtYAZsQ>

Description

this email is claiming to be from "chase Bank" and it is asking the recipient to reactive their account

its claims that the account has placed a tempory suspension

Sender Analysis: Although claiming to be from Chaise Bank but the address from unrelated domain

Additionally the return-path is from "proton.me" witch not affliated with Chase Bank

URL Analysis: After checking the URL using URLscan and VirusTotal it appeared to be clean at the time of analysis

Verdict: This email is identified as a phishing attempt aiming to steal login credentials

Defence Actions: delete the email and do not interact whith it