DON'T GET HOOKED BY PHISHING SCAMS

FROM

- Is the sender unfamiliar?
- Is the email address suspicious or misspelled?

SEND TIME

- Was the email sent early in the morning, as if from a foreign time zone?

SPELLING

- Does the email contain misspellings or poor grammar?

WEB LINKS

- Is the web address a misspelling of a well-known website?
- When you mouse over the link, is the destination address different than the one in the email?

Phishing occurs when hackers try to trick you into revealing personal information or downloading malicious software onto your computer or mobile device. Ask yourself these questions when you receive a suspicious email to keep from being "hooked" by a phishing scam.

From: WellsFarqoSupprot@WellsFarqo.net
To: You@YourEmail.com
Date: January 1, 2019 3:00 AM
Subject: Alert: Online ID has been suspended.

Dear Customer,

Your account needs verification, Suspected Account Activites was found. Weve temporarily disabled your account access. Failure to complete verification in 5days your account will be permenantly closed.

Sign in to your online banking to verify your account.
http://www.wellsfarqo.net/verify

Wells Fargo Support Team

SUBJECT

- Is the subject a reply to an email you never sent?
- Does the subject not match the content of the email?

CONTENT

- Is the email demanding that you do something immediately?
- Does the email threaten consequences if you don't do something?
- Does the email promise a reward in return for your immediate action?

ATTACHMENTS

- Does the email include an unexpected attachment, or one unrelated to the email content?
- Is the attachment an unsafe file type? (The only completely safe file type is TXT.)

575-758-4838 · kitcarson.com

KIT CARSON Internet