DON'T TAKE THE BAIT!

When in doubt, check it out. If an email sent to you has any of these red flags, verify with the sender before clicking on any link or downloading an attachment.

Message Header

Do I know the sender?

Is this from someone I usually communicate with?

Does the sender's email address have a suspicious domain?

Is this an unexpected or unusual email from this sender?

Is the email sent at an odd time, outside regular business hours?

Is the email sent to an unusual group of people?

Is the subject line match the content of the email?

Think Before You Click

You should always take caution when clicking on a link or opening an attachment. Before you click:

1. Hover your mouse over the link and be sure the link address displayed is to a website you'd expect.
2. Take a good look at the web address displayed to be sure it doesn't contain any spelling errors.

From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday, February 3, 16, 05:45am
Subject: Direct Deposit System Update

Sally, You are receiving this email because you have authorized Bank payroll to pay you through direct deposit.

Due to a recent update to system, your direct deposit routing and account number will need to be updated by Tuesday. Failure to do so will result in the loss of direct deposit status and require you to pick up your pay check from payroll each pay period.
Remember to save the direct deposit emails for your records.

To update your direct deposit information please click the link below and verify your account:

Employee Portal

Office of Payroll
Your CEO

Message Body

Is the email written in a style consistent with the sender?

Does the email contain bad grammar, odd styling, or spelling errors?

Is there a link or attachment?

Does the email just seem "off" or give you an uneasy feeling?

Is the sender asking for personal, financial, or customer information?

KansasLand Bank