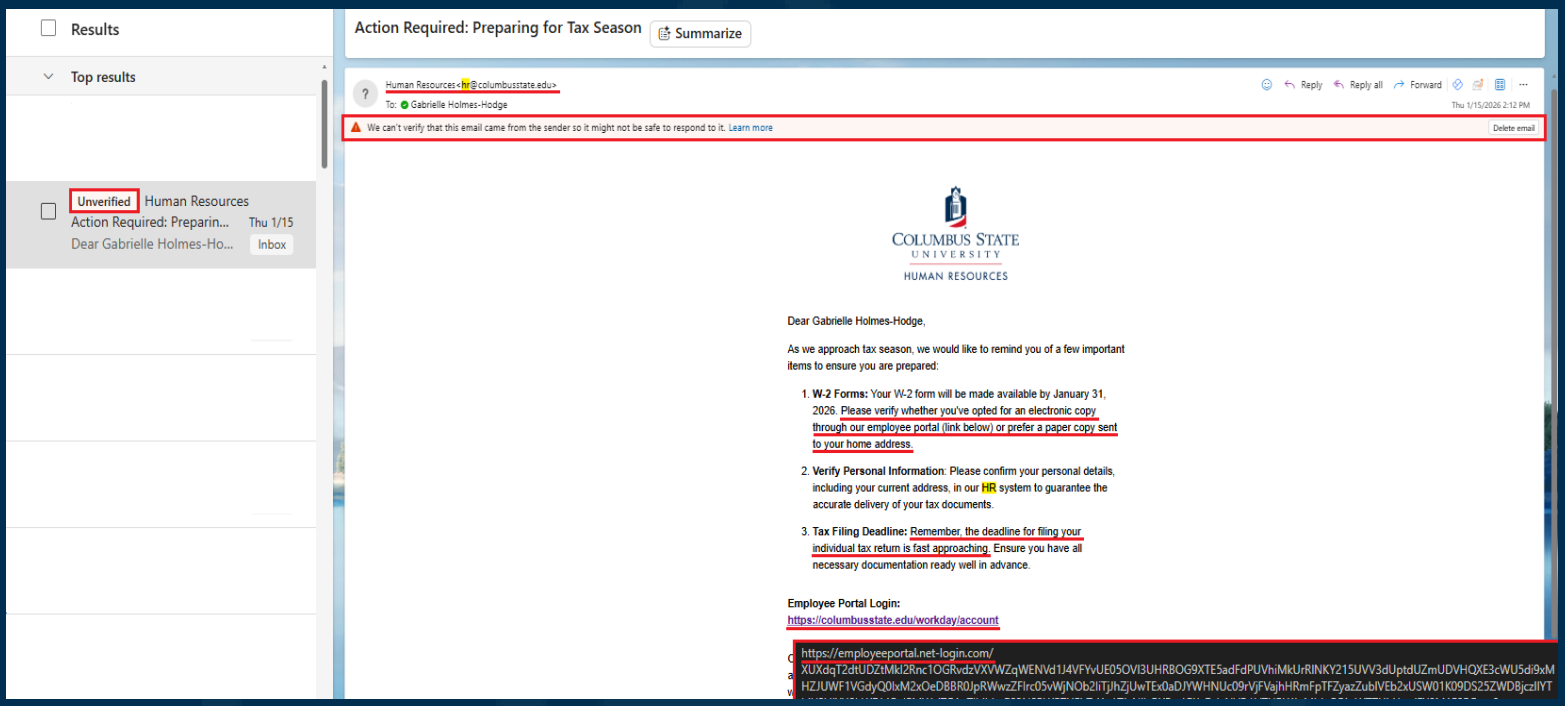
# Phishing Red Flags




## 1. "Unverified Sender"

The first detail that should set off alarm bells was that the email was coming from an **"Unverified"** sender. Microsoft warned that they were unable to verify the sender of the email, and it might not be safe to respond.

## 2. Unusual Appearance

Another red flag was the **inconsistency with typical CSU HR communications**:

- The email did **not** come from CSU's Chief Human Resources Officer.
- The design and formatting, including the text and color scheme, did **not** match CSU's usual HR email style.

## 3. Urgency to Prompting Action

The email attempted to create **a false sense of urgency**, emphasizing a fast-approaching deadline to encourage quick action.

Urgency on its own is not always malicious, but when combined with other red flags, it becomes a strong indicator of phishing.

## 4. Suspicious Link Behavior

Hovering over the link, it's **taking you to a different address than what is shown**. Even the link that is diplayed is suspicious, as **our self-service employee information is managed via the Board of Regents website at OneUSG (oneusgconnect.usg.edu)**, not workday

## Report Suspicious emails

If an email feels "off," don't click it or delete it. **Report it**.

Use the **Phish Alert Button (PAB)** to notify UITS. Internet criminals use a variety of tactics to trick users. Staying alert is essential because **YOU are a crucial line of defense** in protecting CSU's systems and data.