

How to Identify External and Suspicious Emails in Google Mail

Kyle Oliveira - 2025-11-07 - Comments (0) - Email

To protect you from phishing attempts and malicious emails, your Google Workspace account uses several built-in security features. These features provide clear visual warnings to help you identify when you are communicating with someone outside of the university or when an email is potentially fraudulent.

Learning to recognize these visual cues is the best way to prevent falling victim to a spoofed email or phishing attack.

Warnings on Incoming Emails (Receiving Mail)

When you receive an email, pay attention to this visual cue.

The "External" Tag

If an email thread includes any recipients from outside our organization, a yellow "External" tag will appear next to the subject line in your inbox.

- **What it looks like:**

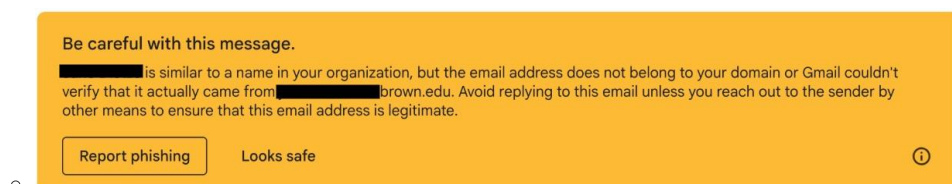


- **What it means:** This is a simple reminder that you are communicating with an external account. Always be cautious when replying, especially with sensitive information.

The "Be careful with this message" Banner (Name Spoofing)

You may see a large yellow warning banner if an email comes from an external sender, but their name is an exact match for someone *inside* our organization.

- **What it looks like:**



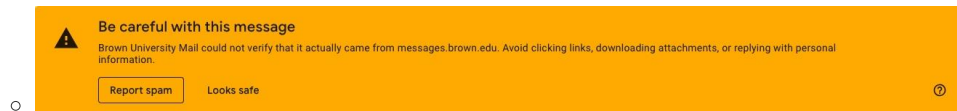
- **What it means:** This is a high-risk warning. It indicates a common phishing technique where an attacker "spoofs" a trusted name to trick you. For example, the sender's name might be "Josiah Carberry," but the email address is community@emaildomain.com, not a university address.

- **What to do:** Do not reply, click any links, or download attachments. If you must, verify the sender's identity through a separate, trusted communication method (like starting a new email or chat). If the email is malicious, click the **"Report phishing"** button.

The "Be careful with this message" Banner (Unauthenticated Mail)

A similar yellow banner will appear if Google cannot verify that an email actually came from the domain it claims to be from.

- **What it looks like:**



- **What it means:** The email is "unauthenticated," and its source is suspicious. You should not trust its contents.
- **What to do:** Avoid clicking links, downloading attachments, or replying with personal information. Use the **"Report spam"** button if it is junk or "Report phishing" if it is malicious.

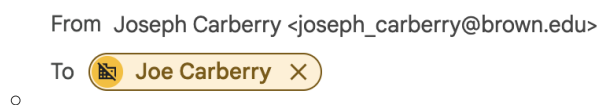
Warnings on Outgoing Emails (Sending Mail)

Warnings also appear when you are *composing* an email to an external person. These are designed to prevent you from accidentally sending sensitive information to the wrong person.

Highlighted External Recipients

When you add an external email address (like a @gmail.com or @outsidebrown.com) to the "To," "Cc," or "Bcc" field, the recipient's name will be highlighted in a yellow tone.

- **What it looks like:**

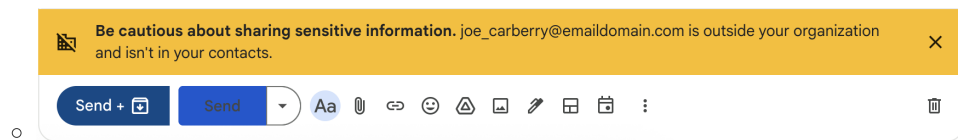


- **What it means:** This visually confirms you are about to send a message outside the organization.

The "Be cautious" Banner

When an external recipient is added, a yellow banner will also appear at the bottom of the email you are composing.

- **What it looks like:**



- **What it means:** This is a final check to ensure you are aware you're sending information externally and to be "cautious about sharing sensitive information." Before clicking "Send," always double-check your recipients' email addresses.