

Gmail Anti-Spoofing Warning Banner

David Boyd - 2020-06-15 - Comments (0) - Email

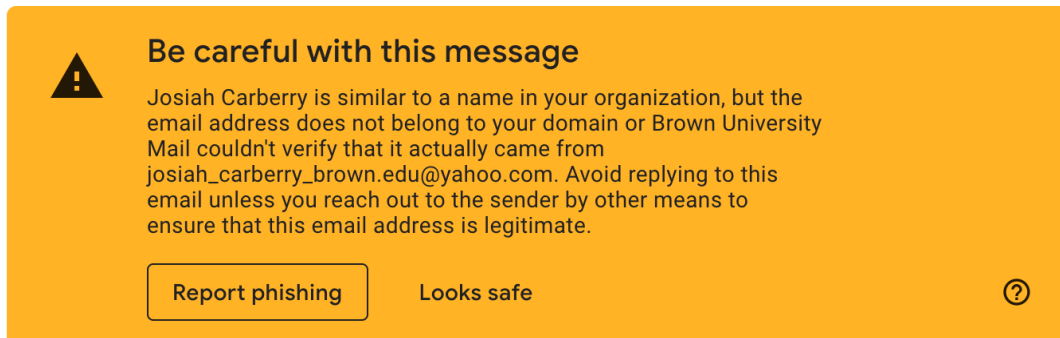
As of June 18, 2020, Gmail may display a warning banner entitled "Be careful with this message" when Google suspects that an opened message is an example of spoofing.

What is spoofing?


Email spoofing is when a message is sent with an impersonated sender address. Spoofing can be legitimate when, for example, an authorized email service is used to send bulk email from a university department email address to students. However, malicious spoofing occurs when an unauthorized or unauthenticated email service is used to send email pretending to be from a university domain, person, or email address.


Spoofing is a component of email [phishing attacks](#), which employ social engineering to trick people into providing sensitive information such as passwords or other data that can be used to compromise identities and systems.

Example of person spoofing:

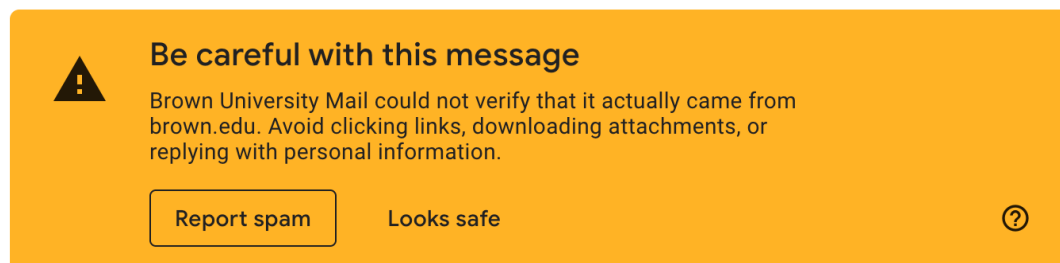


Be careful with this message


 Josiah Carberry is similar to a name in your organization, but the email address does not belong to your domain or Brown University Mail couldn't verify that it actually came from josiah_carberry_brown.edu@yahoo.com. Avoid replying to this email unless you reach out to the sender by other means to ensure that this email address is legitimate.


Looks safe 

Example of domain spoofing:



Be careful with this message

 Brown University Mail could not verify that it actually came from brown.edu. Avoid clicking links, downloading attachments, or replying with personal information.

Looks safe 

How does Gmail protect you from spoofing?

Starting on June 18, 2020, Gmail will display a warning banner when you open a message that Google cannot verify. There are a few scenarios that might trigger these warnings.

1. A message sent from an unauthenticated email domain

2. A message sent from an email domain that is visually similar to brown.edu
3. A message sent from an email address and/or display name that is similar to a brown.edu account (e.g., Josiah Carberry <josiah_carberry_brown.edu@yahoo.com>)

It is important to note that these warning banners are only displayed when viewing opened messages in the Gmail web interface and mobile (iOS and Android) Gmail apps. If you open a suspicious message in a non-Gmail client, you may want to view the message in a Gmail client to see if Google considers it suspicious as well.

What should I do if I see a warning banner?

If you receive a message with one of these warnings, you should proceed with caution.

A sender similar to a name in your organization

You are communicating with someone who is not using a @brown.edu address. This could be someone's personal email address or it could be a spoofing attempt. [Read the message header](#) information closely to be sure.

A message that could not be verified that it came from the domain

Verify whether or not the message is legitimate by contacting the person or company purporting to have sent the message using means other than replying to the message. If the message turns out to be malicious, use the [Report Spam](#) or [Report Phishing](#) buttons in the warning banner to let Google know it should treat that message as such.

What should I do if my identity is being spoofed?

CIS has secured the email domain to help prevent email spoofing, either by blocking such unauthenticated messages or by displaying these warning banners so that recipients will know that a spoofed message is not actually from you.

If you or someone else receive messages that you did not send, especially if Google does not flag them as suspicious, [contact us](#).

What should I do if recipients see a warning banner when opening messages I send them?

Messages you send from the Gmail client using your @brown.edu account should not display a warning banner when recipients open them. However, there are a few scenarios that might trigger these warnings.

1. You send a message to a @brown.edu account using your personal email address
2. You send a message to a @brown.edu account using an email server other than Google's (e.g., Mailchimp) that has not been authorized and authenticated for use with the brown.edu domain.

If the second scenario applies, contact your department IT support staff or the [IT Service Center](#). They will get you in touch with Brown's Gmail administrators to set up authentication, or move your mailing to Brown-run services.

Credit to [UALR ITS](#) for the format and content of this article.