Retrieve Complete Headers from an Email

Last Modified on 08/22/2024 9:50 am EDT

When troubleshooting email problems, we may ask you for the headers of an email to support a technical issue (for example when emails are being blocked by our spam filters or anti-phishing services) or to support a security-related matter.

When you are dealing with an actual suspected phishing attack, Wharton's Information Security Office needs to see the whole message, not just the headers. See the section Forwarding a Message as an Attachment below for advice in these situations.

For more information about headers and their function, see Penn ISC's information on Email Headers.)

Table of Contents:

- Email Headers by Client
  - Gmail
  - Outlook (Windows and Web Client)
  - Outlook (macOS)
  - Apple Mail
- Forwarding a Message as an Attachment
- Questions?

Unfortunately, simply forwarding an email to your Wharton Computing representative will not include the email's original header information. Instead, you'll need to follow the directions linked below for the email client you use to read your email.

Email Headers by Client

Each email client displays their complete headers in slightly different ways. Find your email client and use the links provided for directions on copying email headers.

If you don't see your client listed, see ISC's Email Header section on Other Email Clients.

Gmail

Use this Gmail Help article to help you locate the message header for an email.

Outlook (Windows and Web Client)

Use this Microsoft Support article to help you locate the message header for an email.

Outlook (macOS)

Use these steps to help you locate the message headers for an email: Read More

Apple Mail

Use this Apple Support article to help you locate the message header for an email.

Top

Forwarding a Message as an Attachment

In cases where a phishing email is suspected, we will need the following information in order to fully investigate:

1. In your mail client, **right-click or open the options menu** on the original email.
2. In the menu that appears, select **Forward as Attachment**.
3. A new email will appear with the full message attached as a .eml file attached.
4. Add **security@wharton.upenn.edu** in the "To:" field of that new email and send!

Depending on the type of device you are using, you may also be able to simply click and drag the original email to your desktop to get the .eml file we need - you can attach that in an email to security@wharton.upenn.edu. On iOS/Android mobile mail clients, the menu on the original phishing message should also show a "Forward as Attachment" option; in these cases skip to Step 4 and send.

Top

Questions?

- General Questions - contact your Wharton Computing representative.
- Urgent Security Issues/Questions - contact the Wharton Information Security Office.