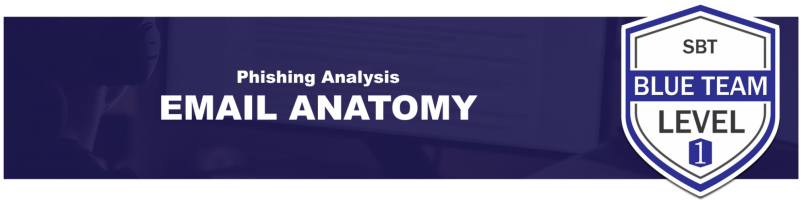
Anatomy of an Email



Ever wondered what actually makes an email? Electronic mail messages are comprised of two parts; a **header** and a **body**. We'll cover both of these parts as it will make it more straightforward when conducting artifact retrieval and analysis in later lessons.

EMAIL HEADER

A header is a set of lines containing information about the message's transportation, such as the sender's address, the recipient's address, or timestamps showing when the message was sent by intermediary servers to the transport agents (MTAs), which act as a mail sorting office. The header begins with the **From** line and is changed each time it passes through an intermediary server. Using headers, you can see the exact path taken by the email and how long it took each server to process.

Header Fields

The **message** itself, made up of the two following elements: the **header fields**, a set of lines describing the message's settings, such as the sender, the recipient, the date, etc. An email includes at least the three following headers:

- **From**, showing the sender's email address
- **To**, showing the recipient's email address
- **Date**, showing the date when the email was sent.

Optional Header Fields

It may also contain the following optional fields:

- **Received,** showing various information about the intermediary servers and the date when the message was processed
- **Reply-To**, showing a reply address
- **subject** showing the message's subject
- **message-ID**, showing a unique identification for the message
- **message body**, containing the message, separated from the header by a line break

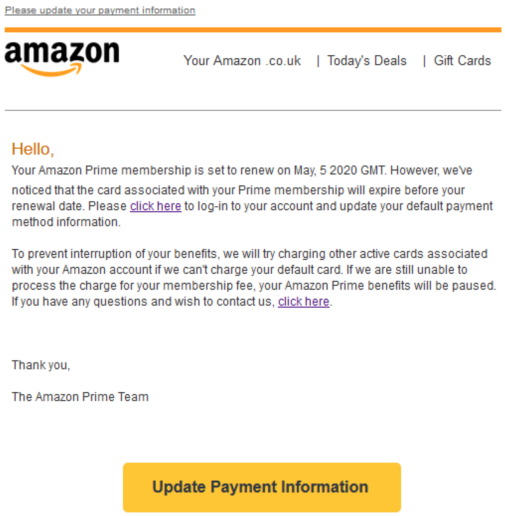
Custom X-Headers

It is important to note that header data is no guarantee of when the message was sent or who sent it, as values can be edited without any requirement for authorization, such as changing the From address to make it look like the email has come from "contact@amazon.co.uk" (We cover Sender Spoofing in more detail in PA3) Tactics and Techniques Used). Additional personalized headers (called **X-headers**) can be set in order to provide the appropriate information. X-headers are called such because their name must begin with **X-**. For example, some anti-spam software programs mark messages as unwanted using the following header: `X-Spam-Status: YES`.

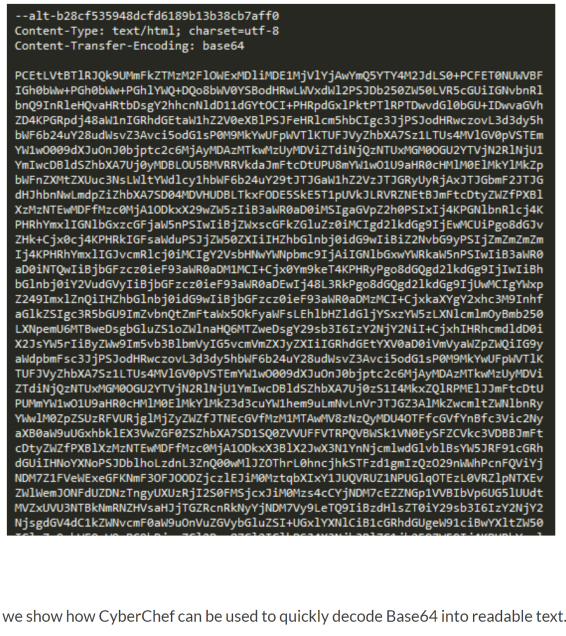
EMAIL BODY

An email body is where the information written by the sender is displayed for the recipient. This can be purely text-based or it can include hyperlinks, images, and HTML styling.

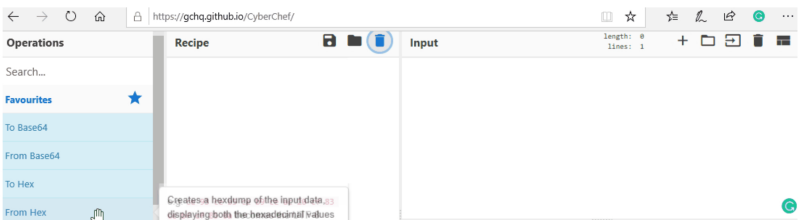
This is the email we're going to walk you through, a fake Amazon email. This email looks genuine and uses Amazon colors and branding to effectively impersonate the brand. The email is structured nicely, and there are no spelling mistakes, improving its effectiveness.

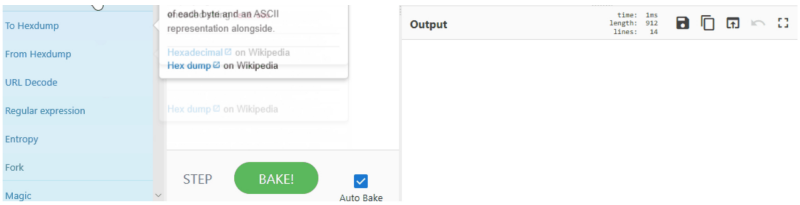


It is fairly common for emails to use encoding for their contents, especially if they are using a lot of HTML styling, as this works to reduce the size of the email. In the below image you can see that we are told on the third line of this screenshot that the email content is encoded in base64. So let's decode it!



In the below GIF, we show how CyberChef can be used to quickly decode Base64 into readable text.





Previous Topic

Back to Lesson

Next Topic