Email Rail

Hyperlinks

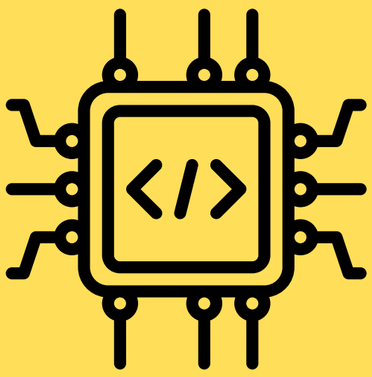
Hyperlinks are the clickable texts in an email that direct you to a website or other online location. Hyperlinks can hide the location you will be sent to on first glance, potentially sending you to a website that will install malware or steal personal information. It is best to hover over hyperlinks to see the full URL before clicking and avoid any hyperlinks coming from unknown senders.

Attachments

Attachments are files sent with an email. This can include documents, images, spreadsheets and more. Malware can be hidden in attachments so it is important to save attachments and scan them with an antivirus before opening them. This includes word documents, PDF's, and other common files; they too can contain malware! Never open an attachment from an unknown sender. Make sure auto-open attachments is turned off to protect your device.

Embedded Images

Embedded Images are pictures that appear directly in the body of the email, rather than being attached. These images can monitor when and where you open the email. To prevent this, turn off HTML mail in email settings. These images can also lead to dangerous sites if clicked on. It is best to turn off automatic image loading in email settings and be cautious of these images that may redirect you to a malicious website.



CISA Sources:

cisa.gov/news-events/news/using-caution-email-attachments

cisa.gov/news-events/news/reducing-spam

Cyber House Rock:

cyberhouserock.info

CISA Information:

cisa.gov/shields-up