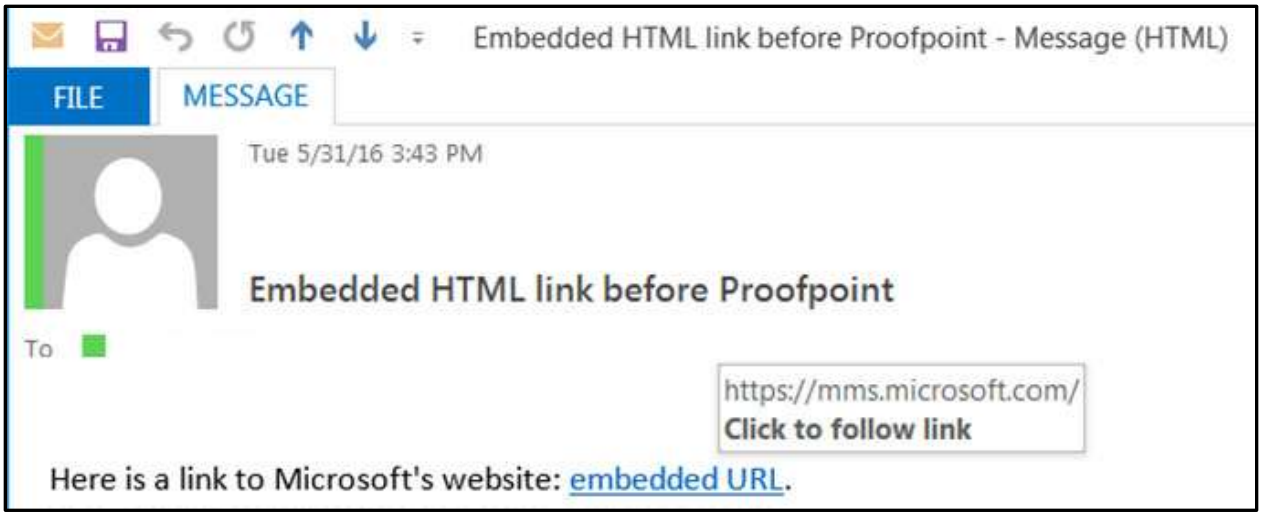
Proofpoint URL Defense

Proofpoint's URL Defense (URL Re-Write) protects you and UT's network resources by blocking access to malicious websites. Links in all email messages are evaluated using a variety of sophisticated techniques to determine the likelihood that they lead back to phishing or malware websites.

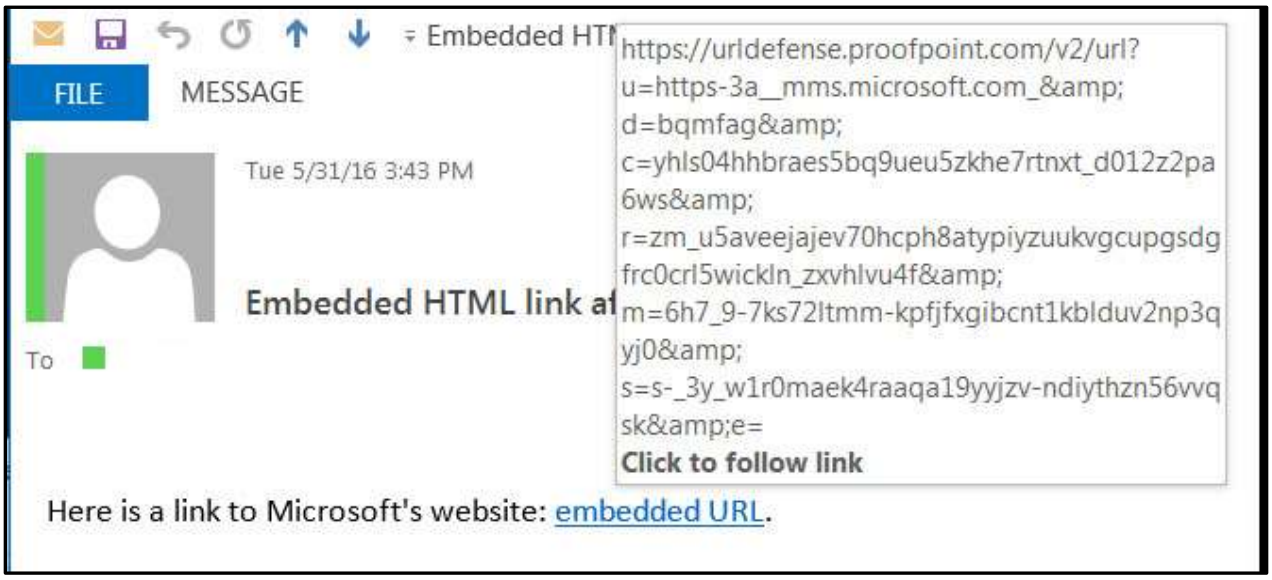
URL Re-writing modifies the links in email messages which directs you to a repository which instantaneously checks the URL for malicious content.

If you hover over the URL you will see *https://urldefense.proofpoint.com/v2/url?=* added to the beginning of the original link following by a string of characters and numbers. If a URL containing phishing or malware is clicked, users will see a message stating that the web page was malicious and blocked. Legitimate sites should load with no delay.

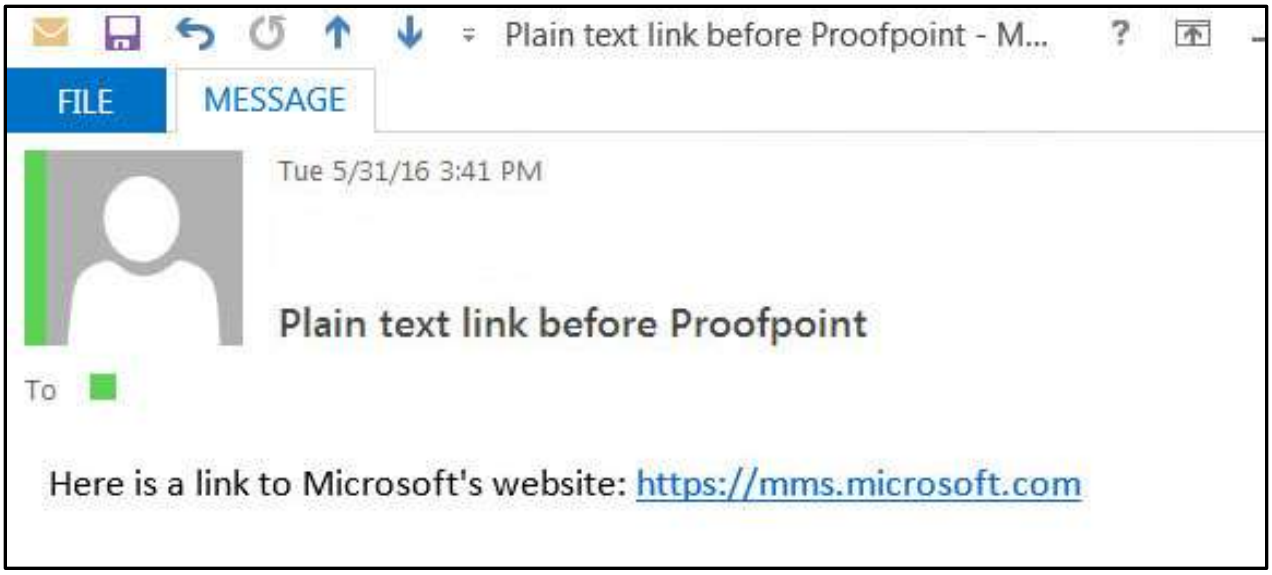
BEFORE URL rewriting--HTML email with an embedded link



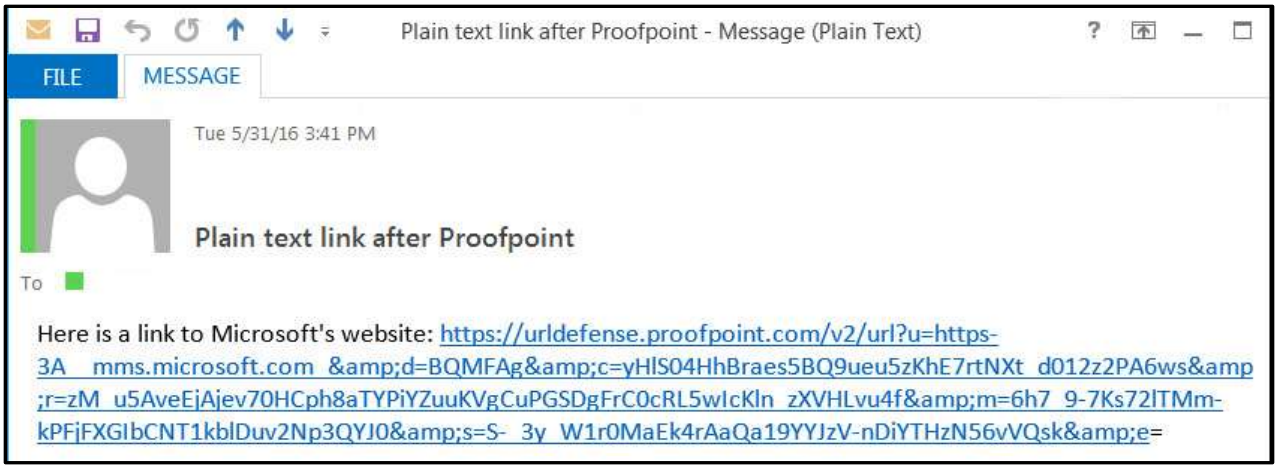
AFTER URL rewriting--HTML email with an embedded link



BEFORE URL rewriting--Plain text email with a link



AFTER URL rewriting--Plain text email with a link



Note: All rewritten URLs will begin with: https://urldefense.proofpoint.com/....

Recent URL threats tend to start out as clean sites so the message passes email SPAM/Phishing/Malware scanning. After messages have been delivered, the site is then updated with malicious information that could compromise your account or systems. Our email security tool, Proofpoint, will check the URL again at the time you click to verify that site is still safe.

If the URL is determined to be safe, you will be immediately directed to the website.

If at the time of your click, the system detects the site to be malicious the following box will appear: