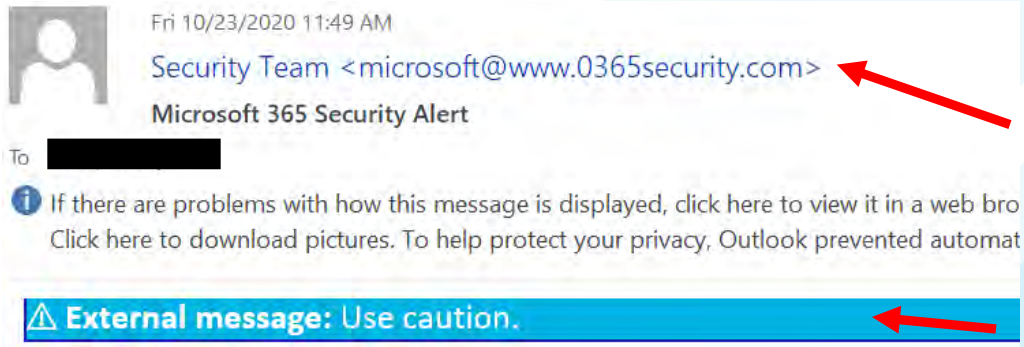
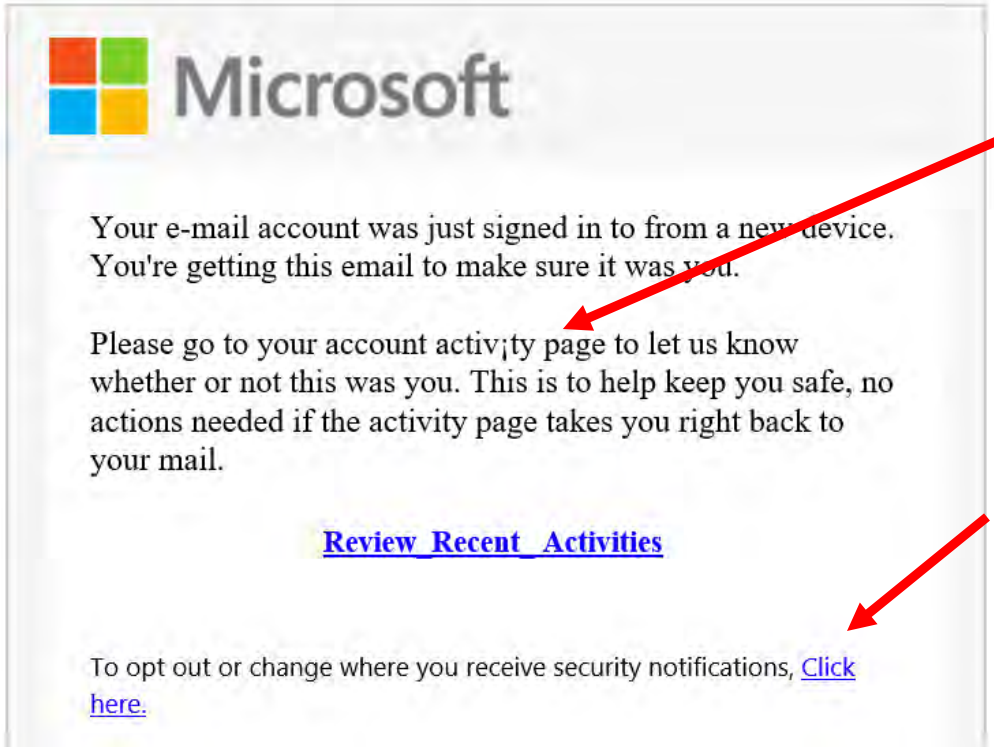
Spot a Phishing Email

Phishing emails can be very convincing. They often include logos and other graphics from legitimate organizations to trick you. In some cases, they may target you by impersonating a service you are already subscribed to. The example below is a typical phish email that appears legitimate at first glance but is actually a phishing attempt. Before you click on links or open attachments within an email, stop and look carefully to verify legitimacy.



***Suspicious "From" address**: A "www" after @ symbol is uncommon. Most Microsoft emails would come from "@microsoft.com"*

***External message flag:** While this is not always an indicator of a malicious email, it does remind you the email is from outside the organization*



***Spelling & Grammar:** There is a spelling error (incorrectly inserted exclamation point). Spelling and grammar issues are often an indicator of phishing attempts*

***Call to Action:** Phishing attempts almost always contain some form of call to action such as an urgent request for reply or request to click on a link*