







Type	Example Feedback	
Points	<div>You stated that this was a phishing email, but it was actually not a phishing email. You received 0 points for this trail</div>	
LLM	<div> <ul style="list-style-type: none"> <li>- The subject "NVIDIA Account Created" is not suspicious.</li> <li>- There is a mismatched link (hovering over it shows "http://nvidia.com/verify/X12K43STP" which is not HTTPS),</li> <li>- There is no urgent language or offers in the email.</li> <li>- The email is asking for account verification but does not directly request credentials</li> </ul> </div> <div>  <div>http://nvidia.com/verify/X12K43STP looks suspicious. Are you sure it's a legitimate address?</div> </div> <div> <div>The URL "http://nvidia.com/verify/X12K43STP" is suspicious partly because it uses HTTP instead of HTTPS, which is less secure. Always look for HTTPS in legitimate URLs. Given no other phishing signs, the email seems trustworthy. Contacting NVIDIA support directly can confirm the email's legitimacy.</div> </div>	<div>   </div>
CLLM	<div> <p><b>**Mismatched Link**</b>: The link text does not match a legitimate Amazon URL ("https://my-to-account-details").</p> <p><b>**Urgent Language**</b>: The email uses urgent language ("fix this quickly", "Don't worry!"),</p> <p><b>**Request for Credentials**</b>: It asks to "Update Your Payment Method Account Details," which is a red flag.</p> </div> <div>  <div>It looks like the sender if from amazon though.</div> </div> <div> <div>Although the sender's address seems legitimate, (cs@accounts.amazon.com) phishing emails often use similar-looking addresses to trick recipients.</div> </div>	<div>   </div>