

**Phishing Traits Found in the Email**

1. **Fake Email Address**
   * The email says it’s from “Amazon Shop,” but the actual email address is do-not-reply@apponline.info.
   * Real Amazon emails come from addresses ending in @amazon.com, not some unknown website.
   * This is a clear sign it’s pretending to be Amazon.
2. **Header Warning**
   * The email shows a warning like: “You are viewing an attached message.”
   * This means the email might have been changed or sent from an unknown or unsafe source.
   * Real emails from trusted companies usually don’t show this kind of warning.
3. **Suspicious Links and Buttons**
   * The email includes buttons like “Sign up for Amazon Prime” and “Product Link.”
   * But these links could actually take you to fake websites that try to steal your login or credit card info.
   * We can’t see the real link in the image, but phishing emails often do this trick.
4. **Dangerous Attachment**
   * The email looks like it contains another message inside (an attached message).
   * This is risky — it might have viruses or try to secretly install bad software on your device.
   * Legit companies rarely send emails with message attachments like this.
5. **Urgent and Tempting Language**
   * It says things like “Sign up now” and “Deals are live!”
   * This creates pressure, making you act fast without thinking carefully.
   * Phishing emails use this trick to make you click links quickly.
6. **Link Text vs Real Link**
   * The visible link might say “Amazon” or “Product Link,” but if you hover your mouse, it might go to a completely different and unsafe site.
   * This trick is used to fool people into clicking.
7. **Spelling and Grammar**
   * The email doesn’t have many spelling or grammar mistakes, which make it look more trustworthy.
   * But even well-written emails can be fake.