**Task 2 - Phishing email analysis for Apple Support scam**

1. **Email Subject:**

* *First checking the email subject was important*

Thanks for contacting us (Apple Support Scam)

1. **Phishing Indicators Identified:**

* *Next was identifying the red flags in the send email. Like the things that makes it known that the email was send as scam*

1. *Generic Greeting Placeholder: -*

Says: Hi {fname}, which is a placeholder. Real emails use your real name.

1. *Suspicious Links: -*

Case link and password reset link may redirect to fake Apple login pages.

1. *Fake Branding: -*

Uses Apple logo and format, but could be easily copied.

1. *Lack of Personalization: -*

No Apple ID, case details, or device info are mentioned.

1. *Trust Language: -*

Tries to sound helpful to lure users into clicking.

1. *Password Reset Trap: -*

Directs users to reset Apple ID, likely to steal credentials

1. **Tools Used:**

* *Finally there was a need to use some tools like a website to check whether the following send email was real email or was it a scam or a phished one*
* *For that we used the tool* [*https://mxtoolbox.com/EmailHeaders.aspx*](https://mxtoolbox.com/EmailHeaders.aspx)

1. **Conclusion:**

This email attempts to impersonate Apple Support using branding and generic placeholders. It includes potentially malicious links and lacks any personal identifiers. This is a strong phishing attempt and should be reported immediately.

1. **References:**

**links**

1. <https://blog.usecure.io/the-most-common-examples-of-a-phishing-email>
2. <https://www.terranovasecurity.com/blog/top-examples-of-phishing-emails>
3. <https://www.hooksecurity.co/glossary/spear-phishing>
4. <https://www.hooksecurity.co/phishing-examples/apple-phishing-example>
5. <https://mxtoolbox.com/EmailHeaders.aspx>
6. <https://support.apple.com/en-us/HT204759>
7. <https://en.wikipedia.org/wiki/Phishing>
8. <https://www.phishing.org/what-is-phishing>