Email Authenticity

Objective:

Provide verifiable information about the origin of email messages by validating the domain ownership of any message transfer agents who participate in transferring and possibly modifying a message.

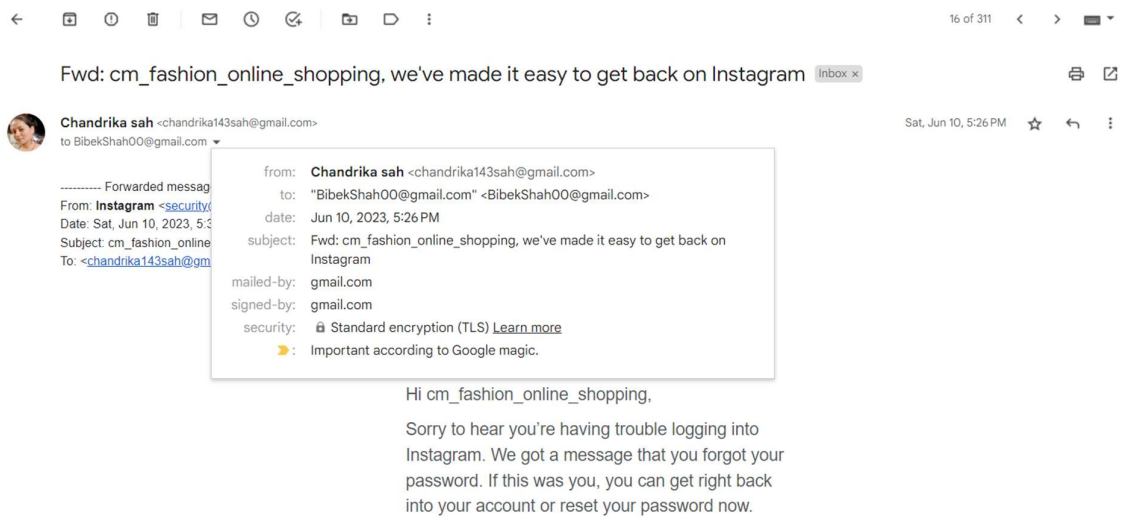
Methodology:

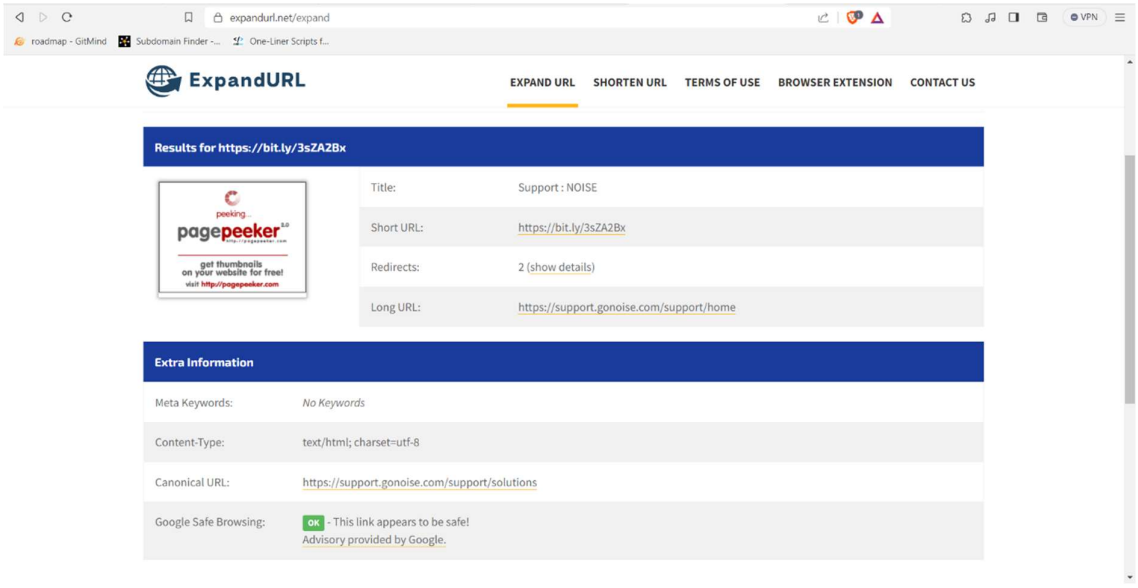
- Checking the main source properly
- Any link within the mail could be suspicious
- Be cautious before clicking on any links
- Scan any suspicious attachments/links before opening

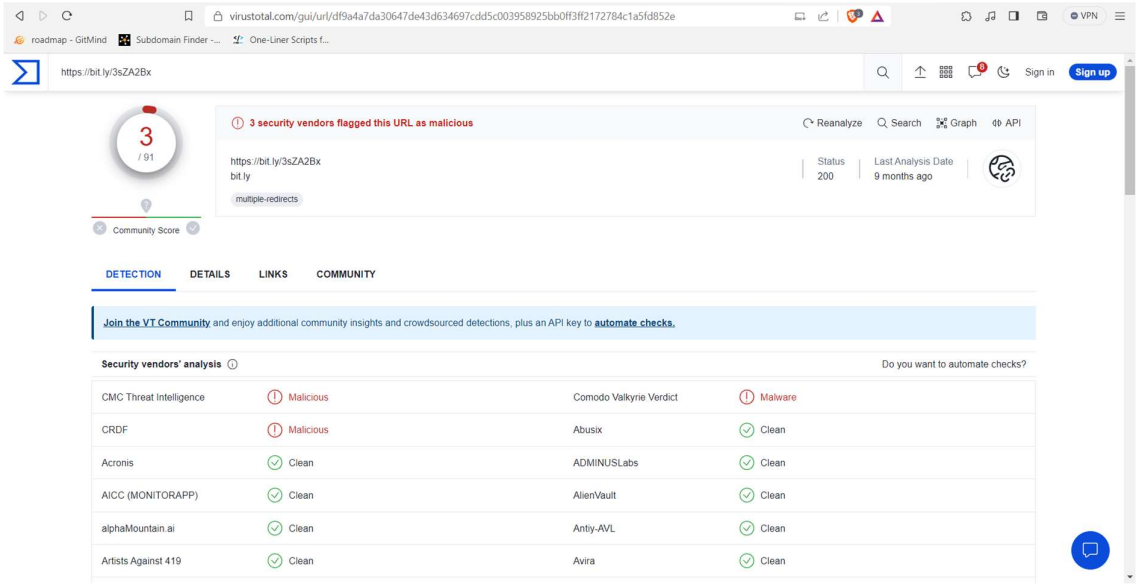
Tools:

- virustotal.com
- expandurl.net

Proof of concept (POC):







Conclusion:

A spoofed mail with a carefully constructed message can be quite a potential threat. It can prove difficult even impossible for an everyday user to identify one as fraudulent.