PHISHING MAIL EXAMPLE

1.Obtain a sample phishing email (many free samples online).

A screenshot of a email

AI-generated content may be incorrect.

2. Examine sender's email address for spoofing.

A type of cyberattack where an attacker disguises their identity to appear as a trusted source, often to trick the victim into revealing sensitive information or taking harmful actions

Annasalai.hp@careind.net

3.Check email headers for discrepancies (using online header analyzer).

A screenshot of a email

AI-generated content may be incorrect.

4.Identify suspicious links or attachments.

Https://bit.lu/2wjyBSZ

<https://www.avast.com/antivirus>

5.Look for urgent or threatening language in the email body.

A screenshot of a email

AI-generated content may be incorrect.

6.Note any mismatched URLs (hover to see real link).

A screenshot of a email

AI-generated content may be incorrect.

7.Verify presence of spelling or grammar errors

A screenshot of a email

AI-generated content may be incorrect.

8.Summarize phishing traits found in the email.

In the above phishing mail , the sender made to believe the receiver that there is a antivirus software that need to update in order to do that the receiver(victim) believed that the mail is a comes from a trusted source.

They mail has been obscured with the URL and the fake antivirus software link to phish the receiver.

Phishing emails aim to trick recipients into revealing sensitive information like passwords or financial details, often by impersonating trusted entities.