Phishing Email Analysis Report

Task 2 – Analyze a Phishing Email Sample

Email Details

- **Subject**: Password reset instructions
- **Sender**: Calendly <calendly@complexity-checker.com>
- **Time Received**: 11:14 AM (25 minutes ago)
- **Recipient**: Demo

Header & Sender Analysis

- **Sender Domain**: complexity-checker.com
    - This does not match the official Calendly domain (calendly.com)
    - This is a red flag indicating domain spoofing
- **Display Name**: "Calendly" – could be spoofed to look legitimate
- **Suspicious behaviour**: Real services use their official domains for password resets

Links and Attachments

- The email contains two clickable links:

  "Reset my password"

  "Click Here" to report unknown request

We cannot verify the actual destination URLs (hover text is not visible in the image), which is typical behaviour in phishing attacks – the links might lead to fake login pages. No file attachments in this case

Email Body Language & Tone

"A request has been made to reset your Calendly account's password… If you did not make this request, please report it"

- Tone Neutral but potentially urgent
- Common phishing tactic: Makes user feel they must take quick action if it wasn't them

Spelling and Grammar

- No spelling or grammar errors found
- However, that doesn't rule out phishing. Advanced phishing emails often have polished grammar to appear legitimate

Summary of Phishing Indicators

Indicator	Description
Spoofed Email Address	Sent from complexity-checker.com instead of calendly.com
Unverified Links	No way to check real URLs from screenshot
Unexpected Reset Request	If user didn’t request it, it's suspicious
Generic Greeting	“Hi Demo” instead of personalized name
Brand Impersonation	Uses Calendly logo and format to appear real