

# PUBLIC NOTICE

## Cyber Security Alert – Phishing & Fake Emails Issued by: IT & HR Departments, HCSSC

In the interest of **Information Security and Data Confidentiality**, the following guidelines are issued for public awareness regarding phishing and fraudulent emails:

### Guidelines for All Recipients

**1 Check the Domain** – Verify that the sender’s domain belongs to HCSSC. If not, treat the email as suspicious.

**2 Do Not Interact** – Do not reply, do not click on links, and do not download attachments from such emails.

**3 Report Immediately** – Any suspicious email must be reported to the IT & HR Departments of HCSSC within 24 hours.

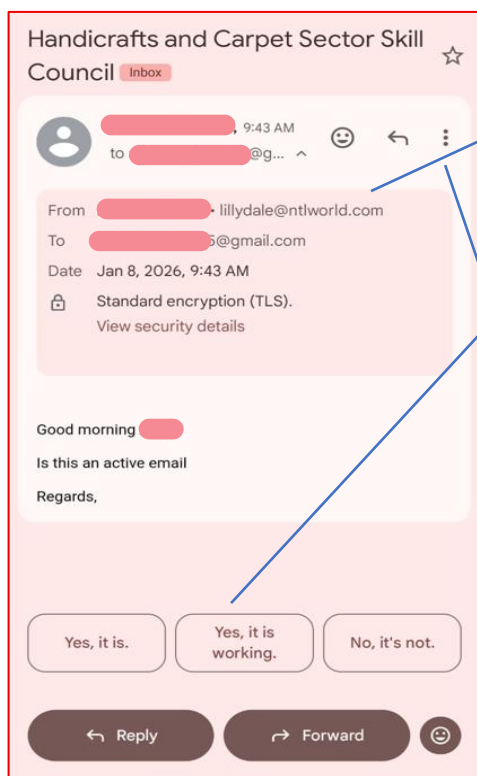
**4 Mark as Spam** – After reporting, mark the email as “Report Spam.”

#### ⚠️ Liability Clause:

Any negligence in following these cybersecurity rules will be the sole responsibility of the concerned party.

🔒 This public notice is issued in the interest of **Information Security & Data Confidentiality of HCSSC**.

Stay alert. Stay safe. Protect your digital identity.



**Step1** – Check Domain  
Not an official HCSSC domain.

**Step2**–Do not reply,  
click links, or download  
files.

**Step3**–Click here to  
report this email.

**Step4**–After informing  
the department,  
mark the email as **“Report  
Spam.”**

