**EMAIL On General Awareness That CISO Can Send His Employees**

**Subject: A Quick Personal Note About Staying Safe Online**

Hi everyone,

I know how busy each of you at {Insert company name}, is juggling multiple priorities every day.   
That’s why I wanted to share some simple, practical tips to help us stay safe online — not just as a company, but for each of you personally.

Cyber threats are getting smarter, and sometimes, they can fool even the most cautious among us. But I trust that with a little awareness, we can all catch them before they cause harm. I’ve seen how vigilant you are, and I truly appreciate your efforts. Let’s keep that momentum going.

Here’s a quick reminder on how to spot a tricky email — truly, it’s often these small details that make all the difference:

* **Watch out for urgent messages** that press you to act immediately, like “Your account will be suspended if you don’t respond now.” Often, scammers try to panic us into clicking before we think.
* **Double-check who sent the email.** Look at the sender’s email address — sometimes it’s very close but just slightly off, like “[support@microsof1.com](mailto:support@microsof1.com)” (with a number ‘1’ instead of an ‘i’).
* **Be wary of unfamiliar links or attachments.** If it doesn’t look right, it probably isn’t.
* **Never share passwords or sensitive info through email.** No trusted company will ask you for your password this way.

**Example from a typical office scenario:**Imagine receiving an email saying, “You have a new document shared on Microsoft OneDrive,” asking you to click a link to view an important report. The email looks professional, but the sender’s address is slightly different, and the link directs you to a site that doesn’t look like our company’s usual Microsoft login page. This is likely a phishing attempt trying to steal your login details.  
If you ever feel unsure, just reach out to our security team. You can email us at [**cybersecurity@company.com**](mailto:cybersecurity@company.com) or call the helpline at **1800-123-4567**. There’s no need to be embarrassed — we’re all learning, and every alert keeps us safer.

Your care and attention make a real difference, not just for the company but for your own digital safety too.

Warm regards,  
[Your Name]  
Chief Information Security Officer