**To:** All Staff Members

**From:** IT Security Department

**Date:** [Insert Date]

**Subject:** Urgent: Protecting Our Organization Against Social Engineering Threats

Dear Team,

We are writing to remind you of the increasing risk of social engineering attacks. Cybercriminals often use deception to manipulate individuals into divulging confidential information or providing unauthorized access to our systems.

To protect our organization, please stay vigilant against the following common tactics:

- **Phishing:** Fraudulent emails that appear to be from trusted sources, asking you to click links or download attachments.
- **Pretexting:** Scammers who create a fake scenario to steal information over the phone or via text.
- **Baiting:** Offers of free items or software that contain malicious code.
- **Business Email Compromise (BEC):** Emails that appear to be from executives requesting urgent wire transfers or sensitive data.

**Best Practices for Protection:**

1. Never share your login credentials or passwords with anyone.
2. Verify any unusual requests for funds or data by calling the requester directly.
3. Do not click on links or open attachments from unknown or suspicious senders.
4. Report any suspicious activity immediately to the IT help desk.

Security is a shared responsibility. Your caution is our strongest defense.

Regards,

[Your Name/Department]
[Organization Name]