Date: [Insert Date]

To: All Staff and Stakeholders

Subject: URGENT: Financial Trojan Threat Mitigation Advisory

Dear Team,

Our cybersecurity monitoring systems have identified an increased risk regarding Financial Trojans targeting corporate banking credentials and sensitive financial data. These malicious programs are designed to steal login information, intercept one-time passwords (OTP), and redirect wire transfers.

To protect our organization's assets, please adhere to the following immediate actions:

- **Email Vigilance:** Do not click on links or download attachments from unknown senders, especially those regarding "unpaid invoices," "account verification," or "urgent payment notices."
- **Browser Security:** Only access financial portals by typing the official URL directly into your browser. Never use links provided in emails or chat messages.
- **Multi-Factor Authentication (MFA):** Ensure MFA is enabled on all financial accounts. Never share your MFA codes or hardware token digits with anyone.
- **System Updates:** Ensure your workstation is running the latest security patches and that your antivirus software is active.

Reporting Suspicious Activity:

If you notice unusual behavior on your computer (such as unexpected pop-ups on banking sites) or suspect your credentials have been compromised, contact the IT Security Department immediately at [Insert Phone Number/Email].

Thank you for your cooperation in maintaining our financial security.

Best regards,

[Your Name/Signature]
[Your Title]
[Department Name]