To: All Department Heads and IT Operations Staff

From: Cybersecurity and Risk Management Division

Date: [Insert Date]

Subject: ADVISORY: Urgent Ransomware Mitigation Protocols for Banking Operations

Dear Team,

In response to the increasing threat landscape targeting financial institutions, this advisory outlines the mandatory mitigation steps to protect our banking infrastructure and customer data from ransomware attacks.

1. Immediate Preventative Measures:

- Enforce Multi-Factor Authentication (MFA) on all remote access points and core banking applications.
- Ensure all critical security patches for operating systems and third-party software are applied within 24 hours.
- Disable unused ports (RDP) and restrict administrative privileges to essential personnel only.

2. Data Backup and Integrity:

- Verify that all transaction logs and customer databases are backed up using the 3-2-1 strategy (3 copies, 2 different media, 1 offline/immutable).
- Conduct a restoration test to ensure backup integrity and recovery time objectives (RTO) are met.

3. Employee Vigilance:

- Report any suspicious emails, unusual login attempts, or slowed system performance to the SOC immediately.
- Do not click on unsolicited links or download attachments from external sources.

4. Incident Response Readiness:

- Review the Ransomware Incident Response Playbook.
- Ensure the emergency contact list for the Incident Response Team and legal counsel is up to date.

Failure to adhere to these protocols poses a significant risk to our operational continuity and regulatory compliance. Please confirm the implementation of these measures with the IT Security Office by [Insert Deadline].

Regards,

[Name]
[Title]
[Bank Name]