To: All Staff and Faculty

From: IT Security Department

Date: [Insert Date]

Subject: ADVISORY: Institutional Phishing Awareness and Cyber Threat Readiness

Dear Colleagues,

This advisory is issued to reinforce our institutional commitment to cybersecurity and to alert you to the increasing sophistication of phishing attempts targeting our organization.

Current Threat Landscape:
Cybercriminals are currently utilizing advanced social engineering tactics, including spoofed executive emails and fraudulent login pages, to steal credentials and gain unauthorized access to institutional data.

Key Indicators of Phishing:

- Urgent or threatening language demanding immediate action.
- Generic greetings or unusual sender addresses.
- Mismatched URLs (hover over links to verify the destination).
- Requests for sensitive information or password resets via email.

Required Actions:

- **Verify:** If you receive an unexpected request for data or funds, contact the sender via a known, secondary communication channel.
- **Report:** Use the "Report Phishing" button in your email client or forward suspicious emails to [Insert Email Address] immediately.
- **Protect:** Ensure Multi-Factor Authentication (MFA) is active on all institutional accounts.

Training and Readiness:
Mandatory cybersecurity awareness training modules will be assigned on [Insert Date]. Completion is required by [Insert Deadline] to ensure our collective readiness against emerging threats.

Thank you for your vigilance in protecting our institution's digital assets.

Best regards,

[Insert Name/Department]
[Insert Organization Name]
[Insert Contact Information]