Personalized Phishing Simulation Results

Date: April 13, 2025 **Employee:** Matthew

Dear Matthew,

This report summarizes your interaction during the recent phishing security simulation.

Your Result Summary

Your Action: You clicked the link in the simulated phishing email. **Status:** `Clicked Link – Remediation Required`

Recommendation: Clicking links in unexpected emails can expose sensitive data or install malware. We strongly recommend completing the assigned security awareness training module on identifying phishing attempts. Please reach out to IT Security if you have questions.

General Security Reminders

- **Verify Senders:** Always check the sender's email address carefully.
- **Inspect Links:** Hover over links (without clicking!) to see the actual destination URL.
- **Beware Urgency:** Phishing emails often create a false sense of urgency.
- **Never Share Credentials:** Legitimate services will rarely ask for your password via email.
- **When in Doubt, Report:** Use the official reporting method if an email seems suspicious.

This is an automated report. Please contact IT Security with any questions.