

Personalized Phishing Simulation Results

Date: April 13, 2025 **Employee:** Hannah Abbott

Dear Hannah,

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

Your Result Summary

Your Action: You did not interact with or report the simulated phishing email. **Status:** Ignored

Recommendation: While ignoring suspicious emails is better than clicking, the safest action is to report them using the official reporting channel (e.g., 'Report Phish' button or forwarding to security@yourcompany.com). This allows our security team to analyze potential threats.

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.