Incident Handler's Journal – #4

Lab Description:

In this lab, I analyzed how phishing attacks are detected and prevented using email security tools. The objective was to learn how suspicious links, attachments, and sender addresses can be identified through automated filters and manual review.

Date: Record the date of the journal entry.	**Entry:** #4 **Date:** October 15, 2025
Objectives	- Identify characteristics of phishing messages and URLs. - Use tools to verify email legitimacy. - Understand the process of reporting and mitigating phishing incidents.
Tool(s) used	PhishTank, VirusTotal, Gmail Security Panel, and WHOIS lookup.
5 W's	Who: Employees within an organization targeted by an unknown phishing campaign. What: A phishing email pretending to be an internal HR message that contained a malicious link.

Findings:	- The sender domain did not match the company's domain. - The link redirected to a fake login portal hosted on a public web server. - The email's IP address originated from an overseas provider unrelated to the organization. - The attachment contained a malicious script flagged by VirusTotal.

	When: During a simulated phishing awareness exercise conducted this week. Where: The organization's corporate email network. Why: To trick employees into clicking the link and entering credentials on a fake login page.
Lessons Learned	- Always verify sender details and link destinations before interacting with emails. - Phishing prevention depends on both user awareness and technical controls. - Automated filters help, but end-user training remains the most effective defense.
Additional notes:	his lab highlighted how phishing remains a major attack vector and how easily users can be tricked by legitimate-looking messages. Continuous awareness, technical defenses, and clear reporting processes are key to reducing the success rate of phishing attacks.