



Cybersecurity (AI) Journal – #5

Lab Description:

In this lab, the objective was to use a generative AI tool to create a reference guide that helps employees identify signs of phishing and malware in emails. The activity demonstrated how AI can streamline cybersecurity education and improve organizational awareness.

Date: Record the date of the journal entry.	Entry: #5 Date: October 20, 2025
Objectives	<ul style="list-style-type: none">- Learn how generative AI can assist cybersecurity professionals in producing educational content efficiently.- Apply the TCREI prompting framework to improve prompt accuracy, tone, and relevance.- Identify and list common indicators of phishing and malware.
Tool(s) used	Gemini (Google AI)
Procedures Used	Began with a simple prompt to generate a phishing-awareness guide, then refined the prompt using TCREI elements such as adding context, audience details, and tone. Evaluated the AI's output after each iteration and adjusted prompts for clarity, depth, and accessibility.
Key Findings	<ul style="list-style-type: none">- Generative AI produces faster educational content but needs clear direction to stay accurate.- Adding context and specifying the audience significantly improves the usefulness of the results.- Iterative prompting yields clearer, better-organized, and more accurate outputs.

Examples of AI-Generated Insights	<ul style="list-style-type: none">- Phishing red flags: suspicious sender addresses, urgent tone, unusual attachments, mismatched URLs.- Malware indicators: unexpected system pop-ups, slow performance, and unauthorized software installations.
Additional Notes	Generative AI should complement not replace security analysts. It's most effective when paired with human review to ensure accuracy and maintain trust in cybersecurity training materials.
