In this activity, you'll leverage a generative AI tool to help you identify common signs of phishing and malware in emails.

This activity is optional and will not affect your completion of the course.

Scenario

You’re working as a cybersecurity professional at a software development company. Recently, employees have complained about receiving a number of phishing emails that attempt to trick them into revealing sensitive information. Your manager has asked you to train the team to better identify phishing emails and signs of malware, which is embedded software designed to harm devices or networks. You decide to create a reference guide for your team. To get started, you ask a generative AI tool to draft a list of the signs of phishing and malware.

Activity tools

In this activity, you will use a browser-based generative AI tool, such as Gemini, ChatGPT, or Microsoft Copilot. Instructions in this activity will refer to Gemini, but you can use the generative AI tool of your choice.

Step 1: Access the template and supporting materials

The following template and supporting materials will help you complete this activity. Keep them open as you proceed to the next steps.

To use the template and supporting materials for this course item, click the following links and select *Use Template*.

* Link to activity template: [Prompt an AI tool](https://docs.google.com/document/d/1AT8P4y6R5oGd_bu-ZYE7uI-3AHJgdLeXwQYLd4IEscs/template/preview?resourcekey=0-rulHUgK_DcQazAXeiZHagQ#heading=h.4n68u9enaw05)
* Link to supporting materials: [Prompt engineering best practices](https://docs.google.com/document/d/1mkB3k5UKhF8oe3usc50nlCkCctorrURD8omVBMClFjE/template/preview#heading=h.9oge1cab2l18)

OR

If you don’t have a Google Account, you can download the template and supporting materials directly from the following attachments.

[Prompt an AI tool](https://d3c33hcgiwev3.cloudfront.net/78XJDMZISoCNTmaHmrMGVQ_a1ac4d0fda5d493da7b07827cbe4b8f1_Prompt-an-AI-tool.docx?Expires=1723852800&Signature=YbMnW872WTrF3hwbPbFMoEtCqKvdsNdx0XqGU5-pX3VbQip-jXFTo00tuiqLp6l2NOnf1KHzV9q~ohABWYJKbfgdUEQdutzzLXXsJ5L0r~7~Sf-Us1DLDjNsF05PqB4R~7YixiSPWFtuuuUdBsuXxImWy-EeiKkYZ4UCzPG7zlQ_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

[DOCX File](https://d3c33hcgiwev3.cloudfront.net/78XJDMZISoCNTmaHmrMGVQ_a1ac4d0fda5d493da7b07827cbe4b8f1_Prompt-an-AI-tool.docx?Expires=1723852800&Signature=YbMnW872WTrF3hwbPbFMoEtCqKvdsNdx0XqGU5-pX3VbQip-jXFTo00tuiqLp6l2NOnf1KHzV9q~ohABWYJKbfgdUEQdutzzLXXsJ5L0r~7~Sf-Us1DLDjNsF05PqB4R~7YixiSPWFtuuuUdBsuXxImWy-EeiKkYZ4UCzPG7zlQ_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

[Prompt engineering best practices](https://d3c33hcgiwev3.cloudfront.net/w8IF30_vSLG1AUTlcdYYBA_d7034b61c44a4d2cbd29de3baaa3b1f1_Prompt-engineering-best-practices.docx?Expires=1723852800&Signature=lHEuPojKvqJVfsEJHCctGZSTMLB0OnHnJDSE-f8-3PZJnrgdGeunCVuwYum0j1lBIBOFKJPvDFx421OgxaGFTzv15VAm~6P6gzwhv7tKjEAltZ~zPP~YkXC4Vc-3RLG300xAAlmi4LWOW3hS2EOBjJhRwptAFMqoAO9FwkFMUDc_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

[DOCX File](https://d3c33hcgiwev3.cloudfront.net/w8IF30_vSLG1AUTlcdYYBA_d7034b61c44a4d2cbd29de3baaa3b1f1_Prompt-engineering-best-practices.docx?Expires=1723852800&Signature=lHEuPojKvqJVfsEJHCctGZSTMLB0OnHnJDSE-f8-3PZJnrgdGeunCVuwYum0j1lBIBOFKJPvDFx421OgxaGFTzv15VAm~6P6gzwhv7tKjEAltZ~zPP~YkXC4Vc-3RLG300xAAlmi4LWOW3hS2EOBjJhRwptAFMqoAO9FwkFMUDc_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

Step 2: Access Gemini

In this activity, you will use a conversational AI tool. You can do this in a browser-based tool like Gemini, ChatGPT, or Microsoft Copilot. Instructions in this activity will refer to Gemini, but you can use the conversational AI tool of your choice.

To access Gemini:

* Go to [gemini.google.com](http://gemini.google.com/).
* Sign in to your personal Google Account.

Refer to the resource about how to [Create a Google Account](https://support.google.com/accounts/answer/27441?hl=en), if you don't already have one. For further assistance signing into Gemini, please refer to [Gemini Apps Help](https://support.google.com/gemini/answer/13278668?hl=en&ref_topic=13194540&sjid=8918468690945255816-NA&visit_id=638435228741836159-1294090182&rd=1).

* For more details on using Gemini, such as who can use Gemini, Gemini’s Privacy Notice, and where Gemini is currently available, refer to the [Gemini Apps FAQ](https://gemini.google.com/faq).
* Please don’t enter private or confidential information in your Gemini conversations or any data you wouldn’t want Google to use to improve its products, services, and machine learning technologies.

Step 3: Prompt Gemini to list signs of phishing and malware

A **prompt** is input that provides instructions to an AI tool about how to generate output. You can prompt Gemini using text or speech and can phrase your prompts in a variety of ways. Your prompt should provide clear and specific instructions that will guide the tool towards generating a targeted response.

To get started, type or speak this prompt or something similar into Gemini:

* *List common signs of phishing or malware that employees can search for.*

Then type or copy and paste your prompt into the **Prompt** section of the **Prompt an AI tool** template.

Step 4: Review the output

Copy and paste Gemini’s output into the **Output** section of the template. Sometimes Gemini offers multiple responses. Choose the one that most closely meets your needs.

Then, carefully review the output to ensure it is factually correct, specific, and detailed enough for your reference guide. As you review the output, consider the following questions:

* Is the output accurate?
* Is the output unbiased?
* Does the output include the information I need?
* Is the output relevant to my project or task?
* Is the output consistent if I use the same prompt multiple times?

Reflect on the ways in which the output meets the goals of your reference guide and how it could better meet your needs. For example, perhaps the tone of the output is formal and you’d prefer something more relaxed.

Then, in the **Notes** section of thetemplate, list at least two ways that the output could better meet your needs.

Step 5: Provide specific follow-up requests

Working to refine your prompts and provide more context can help the generative AI tool produce clearer, more specific, and more useful information. Think of this process as having a conversation with someone, where they tell you something and then you respond by asking for more information or context. Engaging in a back-and-forth dialogue with generative AI tools can lead to more personalized and effective output. And issuing follow-up requests can help produce content that better aligns with your needs.

Review the guidelines in the [Prompt engineering best practices](https://docs.google.com/document/d/1mkB3k5UKhF8oe3usc50nlCkCctorrURD8omVBMClFjE/template/preview#heading=h.9oge1cab2l18) document and refer to the notes you listed in Step 4 about how Gemini’s output could better meet your needs. Then, review the following examples, which demonstrate how a prompt could be iterated upon to produce a more useful output, and implement at least two of these best practices to add follow-up requests to your original prompt:

* **Add a verb.** It's helpful to include a verb in your prompt to produce useful output for your intended task. The provided prompt already includes a verb, but using a different verb like “create” or “construct” would give you a different output.
  + For example: ***List*** *common signs of phishing or malware that employees can search for.*
* **Add context.** Supply more information about the task to help the tool provide better results.
  + For example: *Make this a quick reference guide for professionals who are unfamiliar with cybersecurity concepts.*
* **Add a specific goal**. Include the final goal or specify the outcome that you need. For instance, you could specify that the list of common signs of phishing and malware should only be from a certain period of time.
  + For example: *The guide should teach how to better identify phishing emails and signs of malware.*
* **Reflect on whether you should format your results**. Give specific instructions for how to format the output, such as in a numbered list or ordered by priority.
  + For example: *Provide the response in a numbered list. Order the list by priority.*
* **Provide a persona**. Ask the AI tool to take on the persona of a cybersecurity analyst or another professional in the field. Giving the tool a persona may help it provide specific examples—such as cyberattack activities—within the context of your prompt.
  + For example: *Answer from the perspective of a cybersecurity analyst.*
* **Specify the tone or audience**. Ask the AI tool to tailor its response to a specific audience. You might consider audiences you don’t often interact with, such as senior stakeholders or other relevant audiences.
  + For example: *Rewrite the list for a program manager who has only a basic understanding of cybersecurity concepts.*
* **Supply examples.** Demonstrate the kind of output you’re hoping for.
  + For example, in your prompt, you can provide a list of some common signs of phishing and prompt the AI tool to expand on the list you provide.
* **Specify length.** Ask for a short or long output to give the tool an idea of the desired length of the response.
  + For example: *Refine the list to 10 points or fewer.*

Reflect on the ways in which the iterated output meets your goals. The objective is not to get the perfect output, but to get enough information for you to work with. Be sure to always check your output before using it.

In the **Observations** section of the template, list at least two ways that you iterated on your prompt with follow-up requests and describe how those iterations made the output meet your goals more closely.