

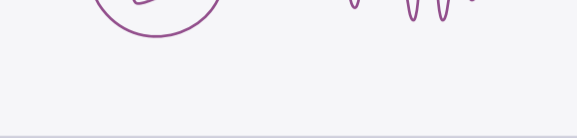
# 8 Prompts to Include in the Custom Instructions of AI Security Mailbox

AI Security Mailbox leverages an AI Security Analyst to provide detailed explanations back to reporters. Security teams can personalize the AI Security Analyst by providing it with custom instructions. What should be included in the custom instructions? The possibilities are endless. Personalizing the AI security analyst to best engage your employees is fun, but when it comes time to type the instructions out it can be difficult. So, for all of you facing writer's block, here are eight customizable prompts to try with your organization!

1

## Specify the Tone

Ultimately you want the interaction with the AI security analyst to be pleasant, engaging, and representative of your security team. Specifying the tone can be an impactful way to accomplish that.



### Potential prompt:

Use a formal tone when communicating with VIPs, but use a professional yet casual tone when communicating with the broader employee base. When responding to reporters who reported an identified malicious email, respond more formally. When responding to reporters who reported an identified safe or spam email, respond with humor.

2

## Create a Custom Template

With the custom instructions box, you can personalize the format of the response emails. This can make the response easier for employees to digest and understand.



### Potential prompt:

Use the following email template when responding to reporters.

Hello {{reporter\_name}},

Thank you for reporting a phishing email and helping keep our organization safe. An automatic analysis of the reported email has been conducted and the email was determined to be {{verdict}}.

Sender: {{sender\_email}}

Subject: {{subject}}

Analysis: {{Insert AI security analysis here}}

3

## Provide Valuable Security Context

Security teams implement policies specific to end users that can be forgotten or misunderstood. Security policies should be included in the custom instructions so the AI security analyst can educate and explain those policies to employees when it makes sense.

### Potential prompt:

We mandate 16 character count passwords, send monthly security awareness training which should be completely thoroughly and promptly, and use [insert vendor name] for MFA.



4

## Encourage Follow-Up Responses

Employees can sustain a conversation with the AI security analyst by responding to the email with additional questions about the reported email or other security-related topics. This creates an opportunity to further educate the employee and improve security awareness.

### Potential prompt:

Include the following at the conclusion of your responses to employees: 'I can help you with additional questions about the reported email or other cybersecurity-related topics. Simply reply to this email with your question!'



5

## Respond in Multiple Languages

If your business operates with employees in several countries, you can customize the AI security analyst to respond in the native languages of those employees.

### Potential prompt:

When responding to employees, begin every response with an English response and then respond with the same message below in French. Separate the English and French responses with a \*\*\*\*.



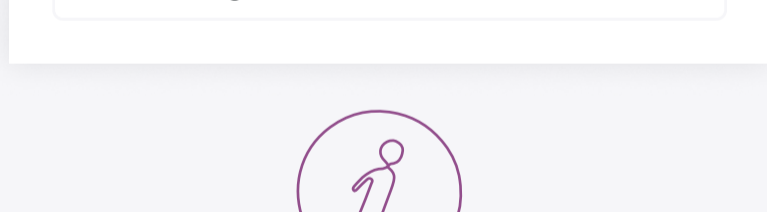
6

## Provide More Verbose Security Awareness Education

AI Security Mailbox capitalizes on the response mechanism to reporters of phishing emails to educate employees. By default, the AI Security Mailbox may include brief tips and tricks on how to identify malicious content, but encouraging more verbose education could capitalize even further on the response motion.

### Potential prompt:

When crafting the response emails, ensure that each message includes a tip on how the reporter can improve their cybersecurity awareness and remain vigilant.



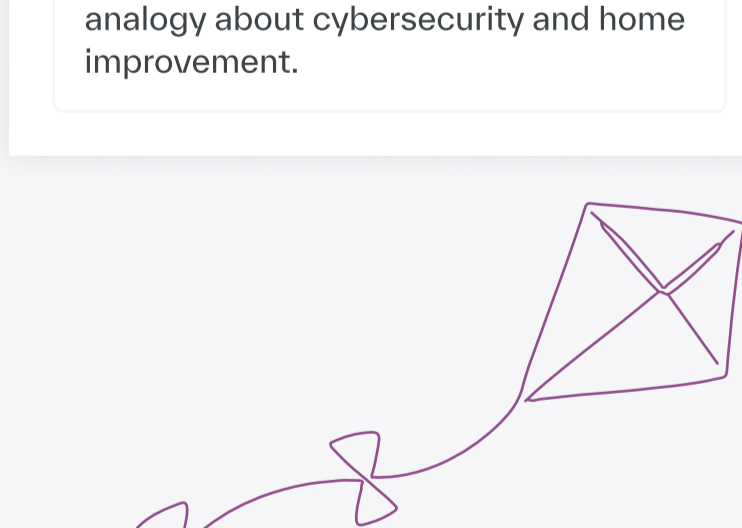
7

## Have Fun with It! Make it Engaging!

Typical interactions between employees and security teams can be challenging, but it's not the fault of the security team! Reminders about training, understanding policies, and updates on MFA or passwords can feel burdensome. The responses sent by the AI security analyst should be fun and engaging and result in a positive experience for the employees. In the example below, I will share a potential prompt that could be used by a home improvement company.

### Potential prompt:

End every response email with a fun analogy about cybersecurity and home improvement.



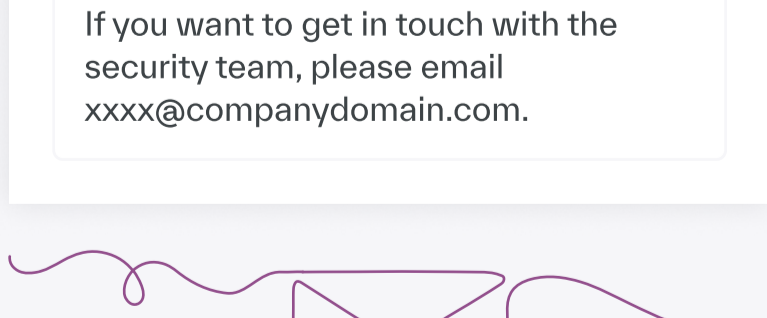
8

## Encourage Reporters to Contact the Security Team

We understand that an AI security analyst might not be useful for every action. In the event that an employee needs a more hands-on response, we recommend providing a medium to request that via the AI security analyst.

### Potential prompt:

End every message with the following: If you want to get in touch with the security team, please email xxxx@companydomain.com.



## Unlock the Power of the AI Security Analyst

"AI Security Mailbox automates the user-reported email workflow 100%, so we don't spend any time on it. The user reports it, and if it's malicious, Abnormal just removes it from inboxes," said Jeff Deakins, Director of Information Security and Infrastructure at Marmon Holdings. "The solution actually does what we need. It's not just about removing malicious emails, which is really the ability to coach and drive security awareness."