Using Artificial Intelligence Securely:

A Guidebook for Secure AI Use in Organizations

Simulate Phishing Threats & Train Your Employees

caniphish

1.

Recognize AI Infallibility

Due to the quality of their training data, AI tools like ChatGPT can be biased, manipulated, or simply incorrect. Human oversight, critical thinking, and verification processes are often necessary to ensure the accuracy and reliability of the information provided by AI systems.

2.

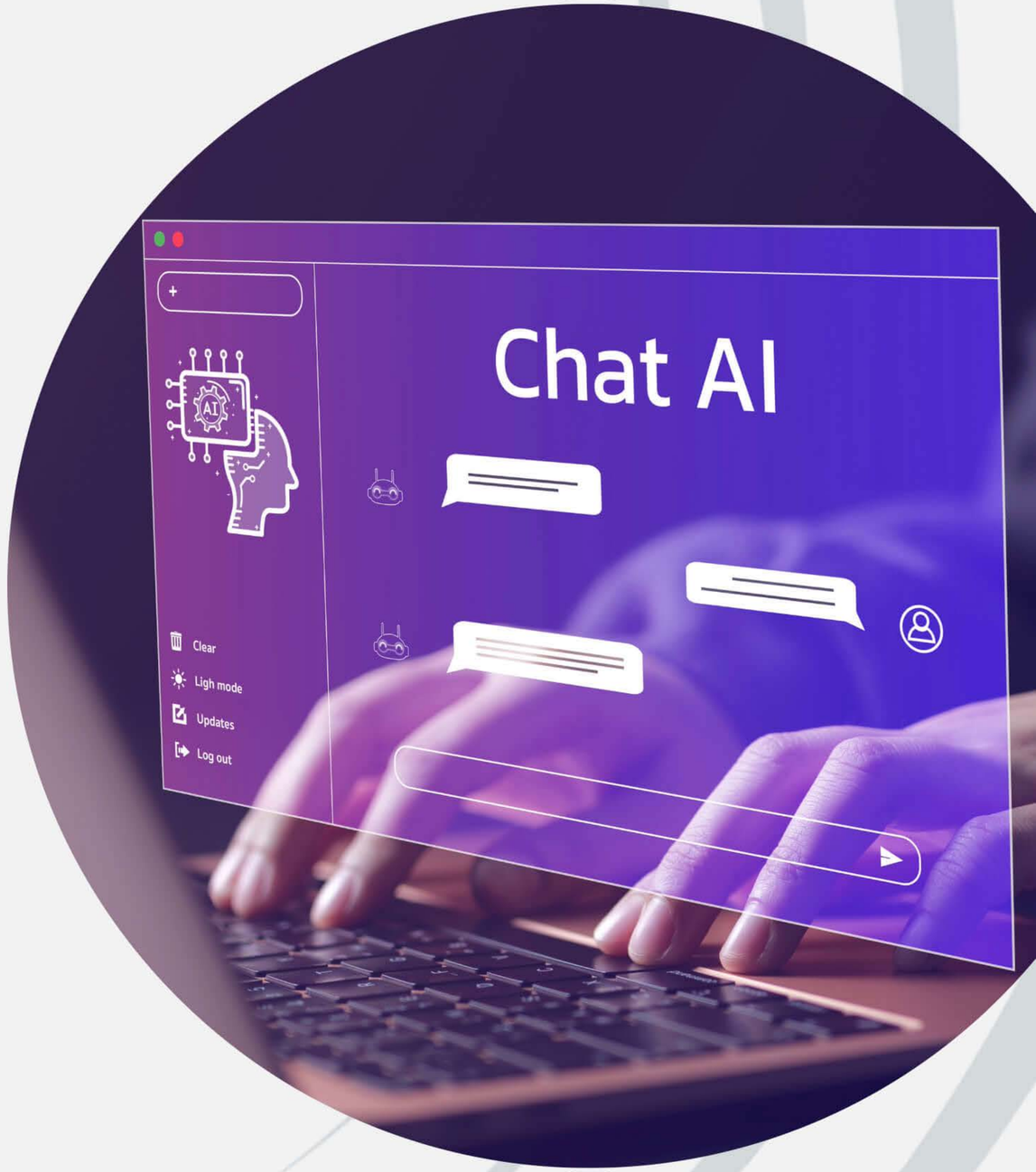
Verify AI Outputs

Whenever you use AI-generated content, especially in critical or professional contexts, independently verify this content before use. Cross-reference with trusted data sources and involve a second opinion or supervisor if necessary to ensure accuracy.

3.

Protect Sensitive Information

Avoid entering sensitive details such as personal identification numbers, proprietary business information, or confidential data with generative AI technologies like ChatGPT or Microsoft Copilot. Once information is input into these systems, it may contribute to the AI's learning database, escaping your control and possibly leading to unintentional exposure.



4.

Use AI Outputs as Preliminary Guides Only

Always regard AI responses as initial guidance, not final answers. Make it a practice to seek additional verification for any critical information provided by AI, fostering a culture of skepticism and diligent verification among your peers.

5.

Recognize and Challenge AI Biases

AI systems, particularly those designed to interact with users, may reinforce existing beliefs by avoiding confrontation. This tendency to agree or not challenge the user's viewpoints can inadvertently contribute to confirmation bias, where users become more entrenched in their beliefs because the AI does not present contrasting views or challenge their assumptions.

Actively question and critically assess AI responses, especially in decisions that affect diversity and inclusion.

Used Securely, AI Is a Powerful Ally

Using AI comes with challenges and risks, especially in a workplace setting. However, when harnessed securely, AI has the power to revolutionize the way we work, interact, and innovate.