KEEPING SAFE WHILE ENGAGING WITH ARTIFICIAL INTELLIGENCE (AI)



Be Mindful of Personal Information: Avoid sharing sensitive personal details. AI applications do not need to know your address, financial information, or proprietary information of the organisation you work for.

Review Privacy Policies: Before using AI applications and services, read the privacy policy of the platform to understand what data is being collected, how data is handled, and who will have access to the data.

Do not Share Passwords or Authentication Details: No legitimate AI application, or institution, will ever ask for your passwords or authentication information. Always keep that a secret!

Understand the Limitations: AI is smart, but it is not perfect. Be aware of its capabilities and limitations and set realistic expectations. Not all results are accurate.

Keep Conversations General: Avoid discussing highly sensitive or confidential matters with AI applications. While some AI models may prioritize privacy, it is always safer to exercise caution.

Be Careful with Links: Be wary of clicking on links generated by AI models. Cybercriminals are using AI in malicious ways to trick unsuspecting victims. Remember the cyber basics!

Use Secure Channels: If you are interacting with an AI application that requires login credentials, ensure that you only log in from a secure connection. Look for the padlock symbol in the address bar and ensure that the URL begins with 'HTTPS://' rather than 'HTTP://.' The 'S' indicates that the webpage has been encrypted and secured with an SSL certificate.

GRANT HUGHES
SPEAKER - AUTHOR - ADVISOR

CyberAwareness
Influencing change, one message at a time