January Tech Tip: Copilot with SSO vs. Public ChatGPT

By: Jennifer Stewart, MPS – ITS Teaching & Learning Product Manager

Understanding Security and Privacy Protections in AI Assistants

Artificial Intelligence (AI) Assistants have become increasingly popular for tasks ranging from document creation to answering questions. Two widely used options are Copilot with Single Sign-On (SSO) integration and the publicly accessible ChatGPT. While both offer powerful AI capabilities, there are important differences in how they protect your data and privacy. This tech tip will help you understand these differences and make informed choices for your workplace or personal use.

What is Copilot with SSO?

Copilot is an AI assistant integrated into Microsoft 365 applications. When used with your UTHSC Single Sign-On (SSO), Copilot authenticates the secure identity provider. This means access is restricted to authorized users, and interactions with Copilot are governed by our enterprise security policies.

What is Public ChatGPT?

ChatGPT, developed by OpenAI, is a conversational AI model available for free to the public via web browsers. Users do not need to authenticate with organizational credentials, and anyone can access the service to ask questions or generate content.

Security and Privacy Protections: Copilot with SSO

- Access Control: Only authenticated users within an organization can use Copilot, reducing the risk of unauthorized access.
- Data Protection: User interactions are protected under the organization's privacy, security, and compliance policies. Sensitive information is less likely to be exposed outside the organization.
- Audit and Monitoring: Organizations can monitor and audit interactions with Copilot, helping to detect and respond to security incidents.
- Regulatory Compliance: Copilot usage can be aligned with legal and regulatory requirements (such as HIPAA, etc.).

Security and Privacy Considerations: Public ChatGPT

- No Access Restrictions: Anyone can use ChatGPT, making it less suitable for sharing confidential or sensitive information.
- Data Exposure Risk: Information submitted to ChatGPT may be processed and stored by the provider. There is little control over how data is used or retained.
- Lack of Compliance: Public ChatGPT does not provide compliance guarantees for regulated industries or sensitive use cases.
- No Organizational Control: There is no way for organizations to monitor or manage how their employees use public ChatGPT.

Choosing the Right Tool for Your Needs

If you need to handle sensitive, proprietary, or regulated information, Copilot with SSO is the safer choice thanks to its built-in security and privacy protections. All faculty, staff, and students have access to a Microsoft 365 Copilot basic account. Log in to your account here to begin your AI journey today.

For casual, non-sensitive queries, public ChatGPT may suffice, but users should exercise caution and avoid sharing confidential information.

If you have any questions, want to explore departmental costs for Pro Account access, or need AI assistance, please submit a request.