Steven Domingo

From:	Kerry Kilber Rebman
Sent:	Thursday, February 6, 2025 4:28 PM
To:	Kerry Kilber Rebman
Subject:	** Tech Bulletin - AI Chats **

Message sent to the following Distribution Lists: Cuyamaca Site, Grossmont Site, District Services

AI Chats: A Public Conversation

Hello, security enthusiasts! We’re excited to bring you another Tech Bulletin on a hot topic: Artificial Intelligence (AI) chatbots. The recent release of the open source chatbot, DeepSeek, has shaken up the AI landscape. ChatGPT and Copilot are no longer the only big teams in the AI playoffs. DeepSeek’s oper source code and significantly lower hardware requirements proves that there is still plenty of room for innovation in AI. This competition for AI supremacy has reached Super Bowl levels of excitement, but amidst all the glamour and glory, the privacy risks of these chatbots are often overlooked.

A recent Forbes article reported a major privacy issue with DeepSeek. A misconfiguration by the DeepSeek team resulted in its database being publicly accessible over the Internet, exposing over one million sensitive records, including chat logs and metadata. Although the DeepSeek team quickly corrected the misconfiguration within an hour of being notified, there is no way to know who accessed th sensitive data while it was exposed. This incident underscores the very real privacy issues associated wi AI.

Remember, AI chats are like conversations in a crowded football stadium. Would you share sensitive information to AI if you know everyone around you could hear? Stay mindful of the risks and protect your privacy with this week’s tips.

This Week’s Tips

- **Avoid entering sensitive information:** Let’s face it: AI is terrible at keeping secrets, so never send sensitive information to AI. At its core, AI was designed to gather data from numerous sources, learn from that data, and generate responses based on that data. Whether sensitive or not, data submitted to AI can b used in responses to other users of the service. So, the next time you decide to have a chat with AI, consic AI like a stranger you just met and ask yourself, “Is this information ok to share with a stranger?”

- **Fact-check the information:** AI may know a lot, but that doesn’t mean it always provides accurate facts Google’s AI once said that parachutes are no more effective than backpacks at preventing major injury whe jumping out of airplanes! False or misleading facts produced by AI have been coined as “hallucinations,” ar it is important to realize that hallucinations exist, and consequences may result from making decisions base on AI responses. Always double-check the information you receive from AI through trusted sources such a academic research, industry experts, or professional organizations.

- **Be aware of biases:** AI algorithms absorb the biases of the Internet and can often produce responses th lean toward certain biases. These biased responses can distort results and lead to dangerous outcomes. F example, Amazon stopped using AI in its hiring process in 2015 when it realized its AI resume tool was usi gender as a factor in ranking job applicants. Know that AI bias is a real problem and not all situations can b safely handled by AI to make fair decisions.

Following these tips can help you to use AI safely and responsibly!

Protect your Password

Important Reminder: Per **AP 3720** at https://www.gcccd.edu/_resources/docs/governing-board/procedures/ch3/ap-3720.pdf, it is your responsibility to never share your network login and password with anyone. District IT will never ask you for your password.

Traveling Outside the U.S. or Mexico?

At the Grossmont-Cuyamaca Community College District, v prioritize the security of our employee and student data. As part of our ongoing efforts, the Information Security department has implemented an out-of-country restriction (excluding Mexico) on access to your GCCCD account. If you plan to travel outside of the U.S. or Mexico and require access to your GCCCD email and account services, please follow the procedures found on the District IT webpage.

Questions? Please contact the District IT Help Desk at **helpdesk@gcccd.edu** or **619-644-7547**.