

Staying Safe on ChatGPT & AI Tools

AI chat tools like ChatGPT boost productivity, but they're not secure places to share sensitive information. Anything entered could be stored, logged, or even exposed. At the same time, attackers are using AI to create more convincing scams than ever.



How Risks Arise



Data Exposure

Information entered into public AI tools may be stored or reused. Sharing confidential company or customer data could put your business at risk.

Tip: *Never paste confidential information into AI tools.*



Unapproved Systems

Not all AI platforms meet company security standards. Using unapproved tools increases the chance of leaks or compliance issues.

Tip: *Only use AI systems approved by your organisation.*



AI-Powered Scams

Attackers use AI to write polished phishing emails, fake documents, and even realistic images or voices. These are harder to spot than traditional scams.

Tip: *Stay alert—AI can make fraud look more legitimate than ever.*



Think Before You Share

AI systems should be treated like public forums, not private databases. If you wouldn't post it on social media, don't type it into an AI tool.

Tip: *Always think twice before sharing information.*