



Staying Secure When Using AI Assistants and Chatbots in 2026

AI assistants can improve productivity, streamline workflows, and help users find information quickly. However, they can also introduce privacy and security risks if used carelessly.

Key Risks

- 1 Sensitive Data Exposure:** Information entered into AI tools may be stored, processed, or shared according to provider policies.
- 2 AI-Enabled Phishing:** Attackers use AI to create more convincing and personalized scams.
- 3 Malicious or Fake AI Services:** Fraudulent AI tools may collect credentials or distribute malware.

Best Practices

- 1 Use Approved AI Tools:** Follow organizational guidance on approved services.
- 2 Never Share Sensitive Information:** Avoid entering passwords, financial data, customer records, or confidential business information.
- 3 Verify AI Responses:** AI-generated content can be inaccurate or manipulated.
- 4 Enable Strong Authentication:** Protect AI accounts with phishing-resistant MFA whenever possible.
- 5 Stay Current:** Keep software, browsers, and security tools updated.



RACE TIP

Treat AI as a helpful teammate, not a source of truth. Always verify critical information.