AI and Information Security

AI best practices that protect both you and your organization.

Treat AI as a Guide, Not a Master

Always verify the sources of information you receive from AI tools. Misinformation can lead to poor decision-making and potential security risks. Cross-check facts with trusted sources to ensure accuracy.

Be mindful of the data you share. Avoid disclosing sensitive or organizational information when interacting with AI systems. This includes passwords, financial details, and proprietary data.

Ensure that your software, including AI applications, is up to date. IT departments often release patches and updates that fix vulnerabilities, making your systems more secure against potential threats.

Tap Your Inner Student

Understanding how AI works, and its limitations can help you recognize suspicious behavior or outputs.

Embrace a culture of security awareness within your organization, where everyone feels responsible for protecting sensitive information.

Only use AI tools that prioritize security and privacy. Look for platforms that offer robust data protection measures and comply with industry standards.

By following these guidelines, you can be a smart, conscientious AI user, effectively protecting yourself and your organization from information security threats.

Barracuda