Cybersecurity & Responsible Practices for AI and LLM Tools

OUTPUT WORKSHOP

✉ hello@output.training
☎ (844) 3OUTPUT

Course Description

This course shows non-technical staff how to use AI and LLM tools safely: what data never belongs in prompts, how to recognize prompt-injection and jailbreak attempts, how to handle file uploads and connectors, how to verify and share outputs, and when to report issues. We also cover basics of vendor/model risk, supply-chain considerations, and light "observability" habits for teams, so everyday users can reduce risk while still getting value from AI. The approach aligns to emerging AI-specific threats and best practices such as lifecycle controls, access governance, and continuous monitoring.

Learning Tracks

Digital Transformation

AI

Business Operations

Compliance

Cybersecurity

Why This Course Matters

- AI introduces new attack paths that traditional security habits don't fully cover; staff need practical guardrails at the point of use.
- "Vibe coding" and self-serve AI tools expand who can build and automate; democratized, easy-to-follow safety practices are essential.
- Clear policies and data-handling rules significantly reduce risk from sensitive data exposure and misconfigurations.

Who Should Attend

Employees who use AI tools

Managers enforcing AI policies

Register Now

COURSE SYLLABUS

Course Overview

Use AI confidently while protecting company data, customers, and intellectual property

What You'll Learn

1. Data minimization for prompts
2. Recognizing prompt injection & jailbreaks
3. Safe handling of files, connectors, & plugins
4. Vendor & model-risk basics
5. Policy, incident reporting, & acceptable use

Syllabus

1. AI Risks 101 for Business Users
2. Data Handling & Minimization for Prompts
3. Recognizing Prompt Injection & Jailbreak Attempts
4. Safe Use of Files, Connectors, & Plugins
5. Output Verification & Sharing
6. Vendor & Model Risk Basics
7. Observability & Feedback Loops for Teams
8. Policies, Governance & the External Landscape
9. Safer Automation & Guardrails
10. Reporting & Continuous Improvement

Register Now

Check out our other courses at:

https://Output.Training