Document Generated: 04/06/2026

Learning Style: Virtual Classroom

Technology:

Difficulty: Beginner

Course Duration: 1 Day

Next Course Date: June 5, 2026

AI Security Essentials for Non-Technical Professionals (TTAI2141)

About This Course:

Artificial intelligence is transforming business operations across every industry, but with this transformation comes new security risks that traditional cybersecurity

approaches cannot fully address. AI Security Essentials for Non-Technical Professionals provides the foundational knowledge needed to understand AI security threats, recognize risks in your organization, and contribute to effective AI security strategies. This course is designed for professionals who interact with AI systems, manage AI projects, evaluate AI vendors, or need to understand AI security implications for their role.

Throughout this intensive day, you will develop a clear understanding of how AI systems work from a security perspective, learn to identify common AI-related threats and vulnerabilities, and understand the human factors that make AI security challenging. You will explore practical scenarios including deepfakes, AI-powered fraud, workplace AI tool usage, and vendor risk assessment. The course emphasizes real-world applications and provides immediately actionable knowledge that participants can apply in their daily work.

With a focus on practical understanding rather than technical implementation, this course provides case studies, demonstrations, and interactive discussions that help participants recognize AI security issues, ask the right questions when evaluating AI solutions, and contribute meaningfully to their organization’s AI security initiatives. Whether you are evaluating AI vendors, managing AI projects, or simply need to understand how AI impacts your organization’s security posture, you will leave with the knowledge to make informed decisions and recognize potential security issues.

Course Objectives:

- Understand AI fundamentals from a security perspective. Recognize what AI systems are, how they work at a basic level, and why they create unique security challenges that differ from traditional IT systems.
- Identify common AI security threats and their business impact. Recognize data poisoning, model manipulation, deepfakes, AI-powered fraud, and other threats that could affect your organization.
- Evaluate AI-related risks in workplace tools and vendor solutions. Ask appropriate security questions when selecting AI tools, understand contract provisions, and assess potential risks from AI implementations.
- Recognize and respond to AI-powered social engineering and fraud. Identify deepfakes, AI-generated content, and sophisticated scams that leverage AI technology to target individuals and organizations.
- Contribute to AI security policy and incident response. Understand your role in AI security, know when and how to report AI-related security concerns, and participate in creating organizational AI usage policies.
- Stay informed about emerging AI security trends. Develop the foundation to understand new AI security threats as they emerge and evaluate their potential impact on your organization.

Audience:

- This beginner-level course is designed for non-technical professionals who need to understand AI security implications in their work. IT professionals, quality assurance teams, project managers, business analysts, security coordinators, and administrative professionals who interact with AI systems or influence AI adoption decisions will gain essential knowledge to contribute to their organization’s AI security posture.

- Entry-level professionals entering IT or software engineering roles, managers overseeing AI projects, procurement professionals evaluating AI vendors, and compliance officers ensuring AI security adherence will also benefit from this foundational understanding. Whether you are directly working with AI systems, managing AI initiatives, or need to understand AI security risks in your organization, this course provides the essential knowledge without requiring technical programming or cybersecurity expertise.

Prerequisites:

- Basic computer literacy and familiarity with common software applications. Comfort using email, web browsers, and standard business applications.

- General understanding of business operations and organizational structures. Awareness of how technology impacts business processes and decision-making.

- Curiosity about technology and willingness to learn new concepts. No technical background required, but openness to understanding how technology affects security and business operations.

Course Outline:

Topic 1: AI Basics - What You Need to Know to Stay Secure

Understanding artificial intelligence fundamentals from a security and business perspective, establishing the foundation for recognizing AI-related risks.

- What is AI vs Machine Learning vs Deep Learning (explained in business terms)
- How AI systems actually work: training data ? statistical models ? predictions
- Critical Reality Check: AI systems are sophisticated pattern-matching and

statistical prediction tools, not thinking entities
- Why AI appears “smart” and conversational but is fundamentally making educated guesses based on training patterns
- Key Insight: The human is the expert making decisions; AI is the assistant providing suggestions based on statistical analysis
- Where AI is being used in your organization: email filters, chatbots, fraud detection, automation
- Why AI security is fundamentally different from traditional IT security

Topic 2: Cybersecurity Fundamentals That Apply to AI

Essential security concepts that everyone should understand, with specific focus on how they apply to AI systems.

- Core security principles: confidentiality, integrity, availability (CIA triad)
- Common attack types: phishing, malware, data breaches, social engineering
- How traditional attacks target AI systems differently than regular IT systems
- Password security, access controls, and data protection basics for AI tools
- Case Study: Real-world examples of traditional security failures affecting AI systems
- Group Discussion: How security breaches in your industry might affect AI systems

Topic 3: AI-Specific Threats You Should Know About

Understanding the unique security threats that target AI systems and their potential business impact.

- Data poisoning: when bad or malicious data creates unreliable AI decisions
- Model manipulation: techniques attackers use to trick AI into wrong answers
- AI system failures and their cascading business consequences
- Supply chain risks: compromised AI models and datasets
- Real-World Examples: Major AI security incidents and their business impact

Afternoon Session

Topic 4: The Human Side of AI Security

Exploring how humans interact with AI systems and the security risks that emerge from these interactions.

- The anthropomorphic illusion: why AI seems human-like and why this creates security vulnerabilities
- Critical Concept: AI assistants provide statistically likely responses, not expert knowledge or factual truth
- The Confidence Problem: AI will respond with equal confidence whether it’s providing accurate information or completely incorrect answers - confidence level doesn’t indicate accuracy

- Understanding AI Hallucinations: When AI generates false information that sounds convincing and authoritative, creating security risks through misinformation
- Social engineering attacks enhanced by AI: deepfakes, voice cloning, sophisticated phishing
- How to spot AI-generated content: text, images, videos, and audio
- Hands-On Practice: Identifying deepfakes and AI-generated content in realistic scenarios
- Protecting yourself and your organization from AI-powered scams and fraud

Topic 5: AI in the Workplace - Opportunities and Risks

Practical guidance for safely using AI tools in professional environments while avoiding security pitfalls.

- Using AI tools safely: ChatGPT, Copilot, image generators, and industry-specific AI applications
- Security Guidelines: What information should and shouldn’t be shared with AI systems
- Intellectual property, confidentiality, and competitive advantage concerns
- Understanding data retention and usage policies for AI services
- Case Studies: Organizations that got AI workplace security right and wrong

Topic 6: Fraud, Deepfakes, and AI Deception

Understanding how criminals leverage AI technology and developing skills to detect and respond to AI-powered deception.

- How criminals use AI for fraud, scams, and identity theft
- Advanced deepfake detection: identifying fake videos, audio, and images
- AI-generated phishing emails and sophisticated social engineering campaigns
- Protecting your organization’s reputation from AI misuse and impersonation
- Interactive Demo: Latest deepfake examples and detection techniques

Topic 7: Building an AI Security Culture in Your Organization

Practical steps for contributing to and promoting AI security awareness within your organization.

- Creating awareness without creating unnecessary fear or resistance
- Establishing practical policies and procedures for AI tool usage
- Your role in AI security: reporting concerns, following guidelines, staying informed
- Training and education strategies for different organizational roles
- Resource Sharing: Tools, websites, and resources for staying current on AI security threats

Course Wrap-Up and Next Steps

- Key takeaways and immediate action items
- Resources for continued learning and staying informed
- How to contribute to your organization’s AI security initiatives
- Q&A and discussion of specific organizational challenges