

## Publication

---

07/28/2025

### AI and Social Engineering Practice Tips

The hospitality industry faces mounting cybersecurity challenges as artificial intelligence (AI) enables increasingly sophisticated social engineering attacks targeting hotels, resorts, and travel service providers. Threat actors now have the capability to leverage AI to craft hyper-realistic phishing emails, deepfake audio messages, and fraudulent booking confirmations designed to deceive employees and guests alike. These evolving threats raise significant legal and regulatory exposure under cybersecurity and data protection laws, such as the FTC Act, state privacy statutes, and international frameworks like the GDPR. This practice tip examines how AI-driven social engineering tactics are reshaping cyber risk in the hospitality sector and outlines key compliance considerations and legal risk mitigation strategies.

#### Why Social Engineering Works

The term “social engineering” was first coined in the late 19th century, but its meaning has evolved significantly over time. As early as the 1980s, the term was being used to describe manipulative techniques used by attackers to deceive individuals into divulging confidential information. These techniques have evolved to include distinct types of “phishing” attacks. In short, attackers send fraudulent emails, texts, or messages that appear to come from legitimate sources, *e.g.*, a bank, a coworker, or IT support, to sidestep cyber controls.

---

#### CLIENT SERVICES

Cybersecurity & Data Privacy  
Hospitality & Leisure  
Intellectual Property

---

#### RELATED PEOPLE

David A. Wheeler

Fine-tuned variants include highly-targeted spear phishing attacks that are often personalized, using data from social media or prior breaches. Whaling attacks target high-profile individuals like executives or legal officers. The goal of such attacks is to trick users into clicking malicious links, opening infected attachments, entering credentials into fake websites, or inducing targets to carry out fraudulent instructions like payment routing. The attacker fabricates a plausible scenario (a “pretext”) to gain trust and obtain sensitive information. For example, an attacker can impersonate a company auditor or IT technician and request login credentials for routine maintenance.

Social engineering works as a cybersecurity attack vector because it targets the most unpredictable system infrastructure element – people. Attackers use deception, manipulation, and psychological tricks to bypass even the most sophisticated technical defenses. Social engineering attacks may be the root cause of 30-40% of recent cybersecurity breaches.

### **AI as a Force Multiplier in Social Engineering**

One of the most concerning developments is the growing intersection between AI and social engineering. From AI-generated phishing emails that mimic human tone with uncanny precision, to deepfake voice and video attacks impersonating executives, these advancements present escalating risks to businesses. Nefarious uses of AI can significantly increase the success rate and scale of social engineering attacks by enhancing an attacker’s ability to personalize, automate, and convincingly mimic human behavior. For example, commercially available large language models enable attackers to create highly personalized phishing emails free of typical grammatical errors or awkward phrasing. AI-generated deepfake voice and video tools can convincingly impersonate executives or IT staff,

increasing the success of attempts to convince individuals to take action that benefits the attacker.

## The Legal Landscape

Individual states remain positioned to be the principal regulators of AI, at least for the near future. The federal budget reconciliation legislation signed into law on July 4, 2025, originally included a 10-year moratorium on state-law regulation of AI. The proposed moratorium was a key subject of congressional negotiations but was removed before the bill's final passage. For now, this means that states will be able to legislate cybersecurity laws with a focus on AI-specific compliance. Based on the lessons learned from state-law consumer privacy legislation, legal compliance will become more challenging.

For example, businesses operating in California and New York or states with similar laws face heightened obligations to safeguard personal data under state-specific cybersecurity and privacy laws. The California Consumer Privacy Act (CCPA), as amended by the CPRA, imposes duties to implement reasonable security measures and provides consumers with rights that, if violated through a breach, may trigger statutory damages. Similarly, New York's SHIELD Act requires businesses to maintain administrative, technical, and physical safeguards to protect confidential information. AI-driven social engineering attacks – such as deepfake customer service requests, impersonated booking confirmations, or AI-enhanced spear-phishing – significantly increase the risk of data breaches and regulatory scrutiny. For hospitality businesses, proactively addressing these evolving threats is not only a cybersecurity best practice, but a legal necessity to reduce liability, maintain consumer trust and comply with the rigorous standards set by the patchwork of various state laws.

## Next Steps for Hospitality Businesses

To mitigate legal and operational risks associated with AI-enhanced social engineering attacks, hospitality organizations should consider taking the following steps:

- **Conduct a Risk Assessment:** Evaluate current vulnerabilities, including susceptibility to phishing, impersonation and credential theft, with particular focus on AI-enabled threats.
- **Update Cybersecurity Policies:** Review and revise data security and incident response policies to ensure compliance with various state data protection laws.
- **Enhance Employee Training:** Implement regular, role-specific training programs to help staff recognize and respond to AI-generated phishing attempts and impersonation tactics.
- **Deploy Advanced Threat Detection Tools:** Invest in AI-driven or behavior-based cybersecurity tools capable of identifying synthetic media, unusual access patterns and spoofed communications.
- **Review Vendor Contracts:** Ensure third-party vendors managing guest or payment data maintain security standards that align with state law and industry best practices.
- **Develop a Deepfake Response Protocol:** Establish procedures for verifying sensitive requests and responding to incidents involving synthetic voice or video impersonation.
- **Engage Legal Counsel:** Work with counsel to stay informed on evolving regulatory requirements and to ensure legal defensibility in the event of a data breach or enforcement action.

## Conclusion



NEAL  
GERBER  
EISENBERG

As AI-powered social engineering tactics become more prevalent and persuasive, hospitality businesses must act decisively to strengthen their cybersecurity posture. Beyond technological safeguards, legal compliance with evolving federal laws like the FTC Act, state laws such as California's CCPA/CPRA, and New York's SHIELD Act demands an initiative-taking, enterprise-wide approach to risk management. Implementing employee training, updating incident response protocols, and conducting regular security assessments are critical steps toward reducing exposure. By staying ahead of these emerging threats, hospitality providers can protect guest trust and operational integrity, while simultaneously meeting their legal obligations in what will be an increasingly complex regulatory environment.

---

*This client alert is part of a series from the NGE Hospitality Industry Team addressing developments and recent news in the hospitality industry.*

*The NGE Hospitality Industry Team is an inter-disciplinary group focused on serving the diverse legal needs of hospitality owners, operators, and investors to achieve their business goals. The group collaborates to ensure our clients are well-informed on industry trends and ready to address both opportunities and challenges.*

*The content above is based on information current at the time of its publication and may not reflect the most recent developments or guidance. Neal Gerber Eisenberg LLP provides this content for general informational purposes only. It does not constitute legal advice, and does not create an attorney-client relationship. You should seek advice from professional advisers with respect to your particular circumstances.*

