

Social Engineering: Don't Get Scammed! Awareness Training and Self-Assessment

Module Number: CPDMI **Module Duration:** 10 - 15 Minutes **Language:** US English

Module Format: OARTeL – On-Demand Assessment and Remediation Tool

Module Overview:

This online training module, which includes 10 self-assessment questions:

- Helps personnel to identify, prevent and react to social engineering threats to the organization to protect against identity theft, privacy breaches and other information security incidents.
- Effectively communicates key information security and privacy issues in just 10 - 15 minutes.
- Engages personnel in critical thinking and decision-making; it does not just feed them information and then ask them to regurgitate the answers in a simplistic quiz as most training modules do.
- Establishes metrics to show where awareness vulnerabilities exist within the workforce
- Provides personnel with pointers to policies and other additional

information that supports effective learning.

“Social Engineering: Don't Get Scammed!” presents the participant with real-life situations to help them gauge the judgment and clarity with which they respond to common types of social engineering attempts. As a result of having personnel complete this program, an organization will be able to assess strengths and weaknesses in their workforce's current understanding of social engineering related threats, meet training compliance requirements, and formulate a strategy for further education.

Scores are broken down into 3 ranges, showing if the participant is proficient, competent, or a novice with regard to understanding social engineering tactics. Numerous references to additional information are also provided to the participants. Organizations

can also include links to their information security and privacy policies within the module. The resulting data will provide your organization with data showing how well your workforce is prepared to deal with social engineering attempts.

This training module also helps organizations meet compliance with a wide range of legal training requirements. For example, in response to new Federal Guidelines, organizations dealing with personally identifiable information (PII) must train employees to identify, prevent and react to social engineering threats to the organization to protect against identity theft, privacy breaches and other information security incidents. HIPAA, GLBA, SOX and many others also require personnel to receive information security and privacy training.

Audience:

Designed for all levels of personnel, including entry level, managers, and executives across the organization.

Participants Will Learn The Three Primary Methods of Social Engineering

- Participants will be able to identify warnings of three primary types of social engineering attempts.
- Participants will be able to prevent successful social engineering attempts.
- Participants will be able to appropriately respond to social engineering attempts.

Rebecca Herold & Associates, LLC, "The Privacy Professor"™ is an information security, privacy and consulting organization providing tools, training, products and consulting to assist organizations of all sizes in all industries worldwide. Rebecca Herold & Associates has received numerous awards, including being named as a Best Privacy Firm and Best Privacy Expert by Computerworld in 2007 and 2008.



Rebecca Herold & Associates, LLC