

Information Security

Along with music and movies, information is increasingly digital, making it easy to transmit and copy — and easy to misuse. While the entertainment industry scrambles to find ways to protect its copyrights, other organizations are likewise struggling to protect their confidential information and to keep pace with the increasingly stringent laws that protect consumer and employee privacy.

Although teenage hackers from faraway countries make the headlines, ordinary breaches of information security often start with things such as an intruder in the workspace, an unscrupulous co-worker or a stolen laptop. A password scrawled on a post-it note under an employee's desk or an un-shredded, discarded memo may be the keys to security breaches that cause grave damage to an organization's financial status and reputation.

Laws such as HIPAA and the Gramm-Leach-Bliley Act demand that employees take specific precautions with certain types of personal information they handle. But even organizations that are not subject to these laws must be sure that their employees understand and follow internal policies for protecting proprietary and/or confidential data in all forms.

Course Summary

This 30-minute course explains the basic principles of information security in simple, understandable terms. It includes pop-quizzes, news clippings and a final quiz highlighting real-world compliance issues that employees should learn to recognize and respond to appropriately.

The topics covered in the program include —

- Information security overview
- Electronic IDs and passwords
- Avoiding identity theft
- Information classification
- Computer viruses and hoaxes
- E-mail and Internet use
- Extra e-mail precautions
- Workspace security
- Social engineering
- Business continuity plans