CAMPUSGUARD®

ONLINE TRAINING
Information Security

CampusGuard's Information Security Awareness Training Course is designed to provide all employees and third parties with access to your organization's computer systems, networks, and information with the knowledge to protect and reduce the risk of sensitive information.

Modules include:

- **Information Security:** This module will discuss what information security is and why it is important to everyone. Training is designed to provide all employees who have access to your organization's computer systems and networks with the awareness and motivation to protect, and reduce, the risk associated with managing sensitive information.
- **Data Classification and Protection:** This module will discuss the classification of sensitive data types and various security and compliance requirements that organizations are responsible for adhering to.
- **Social Engineering:** Statistics continue to indicate that a lack of awareness among employees is the biggest risk facing information security today. This module will review common social engineering attacks so users can more easily identify and protect your organization against potential attacks. Phishing is a major focus of the training with an included sample email with warning indicators highlighted.
- **Email Security**: This module discusses email best practices along with prevention strategies for identifying and avoiding potential risks including spam messages, malicious attachments, and email hoaxes.
- **Password Management**: Strong passwords help to prevent unauthorized access to systems and information. This module covers password best practices, including password strength and management.
- **Remote Work Environments**: This module primarily focuses on remote work environments and understanding the risks and best practices for keeping data and devices secure when operating outside of the corporate environment.
- **Incident Management**: Incident management describes the activities of the organization to identify, analyze, and remediate a potential incident or compromise. This module reviews the different phases of incident management and response and lessons learned from recent breaches.
- **Internal Controls**: Internal controls include all of the policies and procedures an organization uses to safeguard assets, ensure reliability and integrity of information, assure compliance, promote efficient and effective operations, and accomplish operational goals and objectives. This module will review why just having policies in place for acceptable usage, least privilege, etc., is not sufficient alone, and why it is important that all users adhere to them.

- **Security Components:** Technical solutions to address security continue to evolve, and new products and versions are being released daily. This module discusses common components used to secure devices and networks, including firewalls, intrusion detection systems, vulnerability scanning, anti-virus software, encryption, and multi-factor authentication.
- **Physical Security**: If physical access to sensitive information and/or systems is not restricted, unauthorized individuals could easily get their hands on this sensitive data. Best practices for physically securing your environment and basic steps for information storage and disposal are covered in this module.
- **Cyber Crime**: This module reviews some of the most common risks and threats to information systems, like malware, viruses, advanced persistent threats, bots, ransomware, crypto-jacking, and more. Strategies for both proactively protecting systems and devices are discussed, as well as how to identify and report potential compromises.
- **Internet Usage**: This module reviews the importance of using common sense and following information security best practices when accessing the Internet. Topics reviewed include web browsing, cookies, cloud services, file-sharing, and the Internet of Things.
- **Security at Home**: It is important for employees to understand the importance of protecting their home network, and ensuring the right tools are in place before accessing organizational resources. This module also reviews best practices for connecting to networks, installing applications, social networking, and more.
- **Data Breaches and Compromises**: With data breaches continuing to increase, it is critical that organizations understand where the desirable data lives, what the risks are, and limit the risks as much as possible. This module will review some of the weaknesses identified in recent breaches and the average cost of a data breach.
- **Third-Party Risks:** While outsourcing services is chosen for a number of reasons, including increased efficiency, decreased cost, or a lack of internal resources, it doesn't come without risk. This module reviews why it is critical to properly evaluate third-party vendors, understand responsibilities, and implement a program to monitor their compliance on an ongoing basis.
- **Travel Security**: Traveling can pose a significant risk to the information stored on or accessible through laptops, tablets, and smartphones. This module reviews steps to protect employee devices and sensitive information before and during potential business travel.
- **AI Security**: Artificial Intelligence, or AI, if used appropriately, can be a valuable business tool. Applications can be utilized to automate tasks, analyze data, generate reports, and even detect fraud. However, before any AI applications are implemented for organizational use, it is important to understand any associated security risks. This module provides users with an understanding of AI and usage and discusses requirements to ensure AI is used in a way that aligns with industry best practices, privacy and consumer protection regulations, and organizational policies and procedures.
- **Help Desk Security**: Help desks have become a common point of entry for hackers attempting to gain access to organizational systems and/or data. This module provides users with an understanding of social engineering risks targeted at help desk staff, necessary processes for verification of callers, incident reporting and response, how to monitor help desk calls, and best practices for new system updates and/or applications.

Target Audience: All faculty/staff **Course Length:** 8-12 minutes per module; total content 180 minutes

Want to see more? Request a free demo!