BLACK BEAR ACADEMY

CYBER SECURITY AWARENESS

This course is designed to equip employees, business leaders, vendors, and other stakeholders with the knowledge and skills necessary to identify, understand, and mitigate cyber threats. It covers a wide range of topics, including recognizing phishing attempts, understanding social engineering tactics, and implementing best practices for data protection

Agenda: To enhance awareness and understanding of cybersecurity threats, improve personal and organizational security practices, reduce the risk of cyber incidents, and promote a culture of cybersecurity within the organization.

Audience:

- Consultants and Contractors
- Network/System Administrators
- Application Developers
- Management Teams
- Helpdesk and Backoffice Admins

Qualification for This Course

No prior cybersecurity experience is necessary to enroll in this course. The content is designed for anyone looking to enhance their cybersecurity awareness, including employees at all levels who handle sensitive data or work in environments vulnerable to cyber threats.

Professional Growth Opportunities

Completing this course positions individuals to be considered for roles requiring basic cybersecurity knowledge, such as entry-level positions in IT security, or could boost their eligibility for promotions where cybersecurity awareness is valued. It provides foundational knowledge to pursue more specialized cybersecurity certifications or jobs.

Benefits of Certification

By certifying in this course, participants will:

- Demonstrate a proactive approach to cybersecurity, enhancing their professional profile.
- Be better equipped to protect both personal and organizational data, reducing the risk of cyber incidents.
- Gain an advantage in the job market, especially in organizations with a strong emphasis on cybersecurity compliance and awareness.
- Receive a certificate of completion, which can be added to resumes and used in future job applications or performance evaluations.

Session 1 (Morning) - Introduction to Cyber Security Awareness

Objectives: This session will help participants to:

· Understand the fundamental principles of cybersecurity.

· Identify common cyber threats and how they impact organizations.

· Recognize the importance of proactive cybersecurity measures.

· Understand the role of individuals in maintaining cybersecurity.

Topics:

1. Introduction to Cybersecurity

· Definition and Importance

· Overview of the Cybersecurity Landscape

2. Common Cyber Threats

· Phishing, Vishing, and SMShing

· Malware (Viruses, Trojans, Ransomware)

· Social Engineering Tactics

· Business Email Compromise (BEC)

3. Cybersecurity Best Practices

· Creating Strong Passwords and Using Two-Factor Authentication (2FA)

· Secure Browsing and Email Practices

· Identifying and Avoiding Phishing Attempts

· Safe Use of Social Media and Messaging Apps

4. Roles and Responsibilities

· The Role of Individuals in Cybersecurity

· Organizational Policies and Procedures

Exercise: Phishing Simulation and Discussion (1hr)

· Participants will engage in a simulated phishing attack to identify weaknesses and learn how to avoid real-world phishing attempts.

Session 2 (Afternoon) - Building a Culture of Cybersecurity

Objectives: This session will help participants to:

· Recognize the need for continuous cybersecurity awareness and training.

· Understand the importance of incident reporting and response.

· Identify ways to foster a cybersecurity culture within the organization.

· Develop strategies to mitigate risks and protect critical assets.

Topics:

1. Incident Reporting and Response

· Importance of Reporting Suspicious Activities

· Incident Response Procedures

· Collaboration with IT and Security Teams

2. Creating a Cybersecurity-Aware Culture

· Continuous Education and Awareness Programs

· Role of Management in Promoting Cybersecurity

· Engaging Employees in Cybersecurity Initiatives

3. Protecting Critical Assets

· Identifying and Classifying Critical Assets

· Implementing Access Controls

· Data Protection and Privacy Best Practices

4. Emerging Cyber Threats

· Understanding the Evolving Threat Landscape

· Preparing for Advanced Persistent Threats (APT)

· Staying Updated on New Threats and Technologies

Interactive Workshop: Developing a Cybersecurity Action Plan (1hr)

· Requirements: Participants will be divided into smaller groups to brainstorm and develop a cybersecurity action plan.

- Discuss potential cyber threats specific to their roles.
- Create a plan for improving cybersecurity practices in their areas.
- Present their action plans to the group for feedback.

INJECT - Table-Top Exercise: Simulating a Cyber Incident Response (30 mins)

· A simulated cyber incident will be presented, and participants will work through the response process, identifying strengths and areas for improvement.

Reflection:

· What worked well in the incident response simulation? What didn’t?

· What key areas of improvement were identified?

· How can the lessons learned be applied to real-world scenarios?

Lesson to be Learned:

Day 1 establishes the foundation for understanding and implementing effective cybersecurity practices. Continuous learning and adaptation are key to staying ahead of evolving threats.