**IT Department Training and Awareness Plan**

**1. Goals and Objectives**

* **Enhance Cybersecurity Awareness:** Increase employee awareness of cybersecurity threats and best practices to minimize risks.
* **Promote IT Policy Adherence:** Ensure employees understand and comply with IT policies and procedures.
* **Develop IT Skills:** Continuously improve the technical skills of IT staff to maintain system efficiency and security.
* **Foster a Culture of IT Excellence:** Create a positive and collaborative IT culture that prioritizes innovation and problem-solving.

**2. Target Audience**

* **All Employees:** General cybersecurity awareness training.
* **IT Staff:** Technical training on specific software, hardware, and security protocols.

**3. Training and Awareness Programs**

**a. Mandatory Annual Cybersecurity Awareness Training**

* **Phishing Simulations:** Conduct regular phishing simulations to test employees' ability to identify and report suspicious emails.
* **Security Awareness Workshops:** Organize interactive workshops to cover topics like password security, social engineering, and data privacy.
* **Online Training Modules:** Provide accessible online modules on cybersecurity best practices, tailored to different roles and skill levels.

**b. Regular IT Skills Development**

* **Technical Training:** Offer regular technical training sessions on new technologies, software updates, and system administration.
* **Certification Programs:** Encourage and support employees in pursuing industry certifications (e.g., CompTIA, Cisco, Microsoft).
* **Mentorship and Coaching:** Establish a mentorship program to foster knowledge sharing and career development.

**c. Continuous Learning and Development**

* **IT Newsletters:** Distribute regular newsletters with industry news, best practices, and security alerts.
* **Knowledge Sharing Sessions:** Organize internal knowledge-sharing sessions to discuss challenges, solutions, and innovative ideas.
* **External Training and Conferences:** Encourage participation in industry conferences and workshops to stay updated on emerging trends.

**4. Training Delivery Methods**

* **In-Person Training:** Workshops, seminars, and hands-on training sessions.
* **Virtual Training:** Online webinars, virtual classrooms, and self-paced e-learning modules.
* **Hybrid Training:** A combination of in-person and virtual training to cater to diverse learning styles and geographical locations.

**5. Evaluation and Measurement**

* **Pre- and Post-Training Assessments:** Measure knowledge retention and skill improvement.
* **Phishing Simulation Results:** Track employee performance in identifying and reporting phishing attacks.
* **Incident Reporting:** Monitor incident reports to assess the effectiveness of training in preventing security breaches.
* **Employee Feedback Surveys:** Gather feedback on training programs to identify areas for improvement.

**6. Addressing Overseas Locations**

* **Time Zone Considerations:** Schedule training sessions at times convenient for all locations.
* **Language and Cultural Differences:** Provide training materials and conduct sessions in appropriate languages and cultural contexts.
* **Remote Training Tools:** Utilize robust remote training tools to ensure effective delivery and engagement.
* **Regular Communication:** Maintain regular communication with overseas teams to address any training-related concerns or questions.
* **Local laws Training:** Train all employees local laws that may affect their work

By implementing this comprehensive IT training and awareness plan, the e-commerce company can significantly enhance its cybersecurity posture, improve employee skills, and foster a culture of IT excellence.