**Phishing Awareness Training Report**

## Module Title

**Phishing Awareness Training – Detection, Prevention, and Best Practices**

## Short Description (350 characters)

This module educates users on identifying and avoiding phishing attacks. It explains how to recognize phishing emails, fake websites, and social engineering tactics. Includes real-world examples, prevention tips, and interactive quizzes to enhance awareness and protect against online threats.

## Extended Description – Step-by-Step Breakdown

### 1. Understanding Phishing

Phishing is a cyberattack where attackers impersonate legitimate entities to steal sensitive information. Recognizing phishing attempts is crucial for online safety.

### 2. Types of Phishing Attacks

* **Email Phishing**: Fraudulent emails mimicking trusted organizations.
* **Smishing**: Phishing via SMS messages.
* **Vishing**: Voice phishing through phone calls.
* **Spear Phishing**: Targeted attacks on specific individuals.
* **Pharming**: Redirecting users to fake websites by manipulating DNS settings.

### 3. Social Engineering Tactics

* **Pretexting**: Creating a fake scenario to extract information.
* **Baiting**: Offering something tempting to lure victims.
* **Impersonation**: Pretending to be someone trustworthy.
* **Tailgating**: Following someone to gain unauthorized access.

### 4. Best Practices

* Avoid clicking on suspicious links.
* Do not share personal information via email.
* Use two-factor authentication (2FA).
* Verify URLs before entering sensitive information.
* Report phishing emails to authorities.

### 5. Interactive Quiz

A quiz tests users’ understanding with multiple-choice questions based on real-world scenarios, reinforcing learning.

## Visual Aids and Screenshots

* Types of Phishing Attacks diagrams.
* Real-world phishing examples screenshots.
* Interactive quiz interface snapshots.

## Output and Results

* Users learned to identify phishing emails and websites.
* Improved understanding of social engineering tactics.
* Increased confidence in reporting suspicious activities.