Creating an online training module on phishing attacks involves several key elements to ensure it’s interactive, informative, and effective. Below is a detailed outline for an online training module about phishing awareness. This format can be adapted to platforms like **Articulate Storyline**, **Adobe Captivate**, **LMS systems**, or even email-based campaigns.

**Phishing Awareness Online Training Module**

**Module Overview**

**Objective**: The goal of this training is to educate users on recognizing and avoiding phishing attacks, including phishing emails, websites, and social engineering tactics. By the end of the module, users should be able to:

* Identify common signs of phishing emails.
* Recognize phishing websites.
* Understand social engineering tactics used in phishing.

**1. Introduction to Phishing Attacks**

* Interactive Element: An animated video or slideshow explaining what phishing is and why it’s important to be aware of it.
* Content:
  + Phishing is a type of social engineering attack where attackers impersonate legitimate entities to steal sensitive information (e.g., usernames, passwords, financial data).
  + Phishing is often delivered via email, but it can also be conducted through phone calls, text messages, or fake websites.

**2. Types of Phishing Attacks**

* **Interactive Element**: A clickable infographic or animation to reveal different phishing attack types.
* **Content**:
  + **Email Phishing**: Fraudulent emails that seem to come from trusted sources.
  + **Spear Phishing**: Targeted phishing aimed at specific individuals or organizations.
  + **Whaling**: A type of spear phishing targeting high-profile individuals (e.g., CEOs).
  + **Smishing**: Phishing attacks using SMS messages to trick victims.
  + **Vishing**: Phishing through phone calls, pretending to be from a legitimate source.

**3. How to Spot Phishing Emails**

* **Interactive Element**: Simulated phishing email examples where users can click on different parts of the email (subject line, sender’s email, links, attachments, etc.) to learn how to spot red flags.
* **Content**:
  + **Suspicious sender**: The sender’s email address may look similar but not exact.
  + **Urgency or threats**: Phishing emails often contain alarming messages (e.g., "Account suspended" or "Immediate action required").
  + **Generic greetings**: They may say "Dear Customer" instead of using your name.
  + **Suspicious links or attachments**: Hover over links to check if they lead to a legitimate website, and be cautious with attachments.
  + **Grammar and spelling mistakes**: Phishing emails often have poor grammar and odd language.

**4. Real-World Phishing Email Examples**

* **Interactive Element**: A drag-and-drop activity where users match phishing emails to legitimate ones.
* **Content**:
  + Show real-world examples of phishing emails, including visual cues like:
    - A fake bank email asking for login details.
    - An email impersonating a tech company asking you to reset your password.
    - A fake package delivery notification.
  + Users are tasked with identifying phishing characteristics in these emails.

**5. Identifying Phishing Websites**

* **Interactive Element**: A clickable simulation of a phishing website where users are asked to spot clues indicating that the website is fake.
* **Content**:
  + **URL discrepancies**: Fake websites often use URLs that are similar but slightly altered (e.g., "paypal-secure-login.com").
  + **HTTPS**: Look for "HTTPS" in the web address and a padlock symbol.
  + **Poor design**: Phishing websites often have low-quality graphics, broken links, or poor grammar.
  + **Fake login forms**: These sites may ask for your login credentials for legitimate services.

**6. Social Engineering and Phishing**

* **Interactive Element**: A branching scenario where users make decisions based on a simulated conversation with a potential attacker (e.g., phone call or text message).
* **Content**:
  + **Pretexting**: The attacker pretends to be someone you know to trick you into providing sensitive information.
  + **Baiting**: The attacker offers something enticing, like a free prize, to get you to click on a malicious link.
  + **Impersonation**: Attackers may pretend to be customer support or an executive to gain your trust and steal information.
  + **Example**: A phone call from someone claiming to be from IT support, asking you to share your login credentials to "fix an issue."

**7. How to Protect Yourself from Phishing**

* **Interactive Element**: A checklist activity where users tick off actions they should take to protect themselves.
* **Content**:
  + **Don't click on suspicious links**: Always hover over links to see where they lead before clicking.
  + **Verify the source**: If you receive a suspicious email or message, verify its authenticity by contacting the organization directly.
  + **Enable Multi-Factor Authentication (MFA)**: Protect accounts with MFA to add an extra layer of security.
  + **Keep software updated**: Ensure that your antivirus, operating system, and apps are up-to-date.
  + **Educate others**: Share what you’ve learned with colleagues, friends, and family.

**8. Reporting Phishing Attempts**

* **Interactive Element**: A simulated phishing attempt that the user must report.
* **Content**:
  + **Steps to report phishing**:
    - Report to your organization’s IT team.
    - Use the "Report Phishing" option in your email provider.
    - Report suspicious websites to Google Safe Browsing or other relevant platforms.
  + **Example**: A button to "Report" the phishing attempt that leads to a mock reporting page.

**9. Phishing Quiz**

* **Interactive Element**: A short quiz with multiple-choice questions to reinforce the concepts learned.
* **Content**:
  + **Questions**:
    - What are common signs of a phishing email?
    - How can you identify a phishing website?
    - What should you do if you receive a suspicious message?

**10. Conclusion and Certificate**

* **Interactive Element**: Provide a completion certificate once the user passes the quiz.
* **Content**:
  + **Recap**: Remind users of the key takeaways from the course.
  + **Encouragement**: Encourage learners to stay vigilant and share their knowledge with others.
  + **Downloadable Resources**: Provide a downloadable phishing awareness checklist or reference guide.