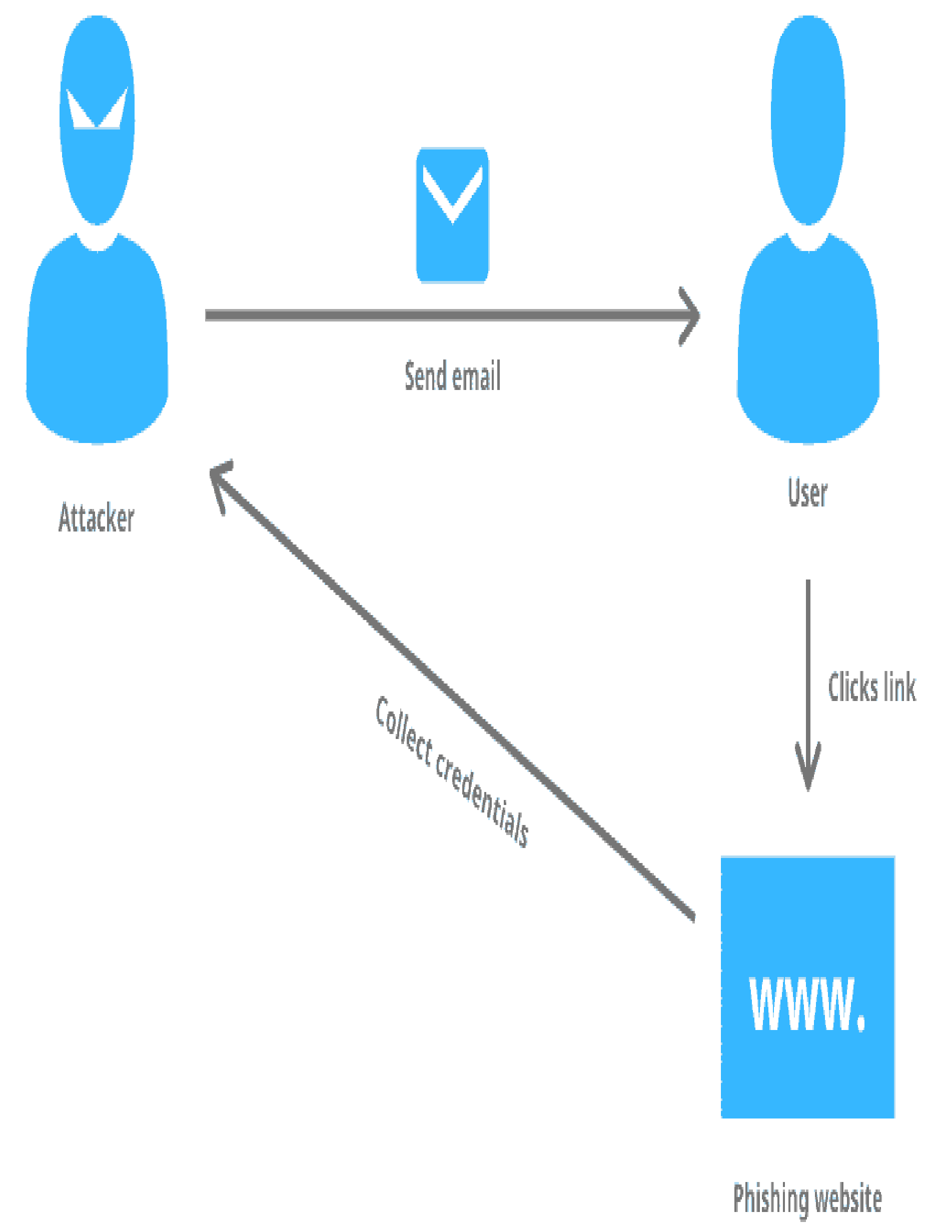
PHISHING AWARENESS TRAINING MODULE

INTRODUCTION TO PHISHING

>Content:

- **Definition of Phishing:** Phishing is a type of social engineering attack where attackers impersonate legitimate organizations to trick individuals into revealing sensitive information such as login credentials, personal details, or financial data.
- **Importance of Awareness:** Phishing attacks are one of the most common and effective methods used by cybercriminals to steal sensitive data and compromise security.



TYPES OF PHISHING ATTACKS

>Content

1.**Email Phishing**: Fraudulent emails that appear to come from trusted organizations, such as banks or service providers.

2.**Spear Phishing**: A more targeted form of phishing, where attackers tailor their emails to specific individuals or organizations.

3.**Whaling**: A type of phishing that targets high-level executives (C-level), often involving highly personalized emails.

4.**Smishing**: Phishing attacks via text message or SMS.

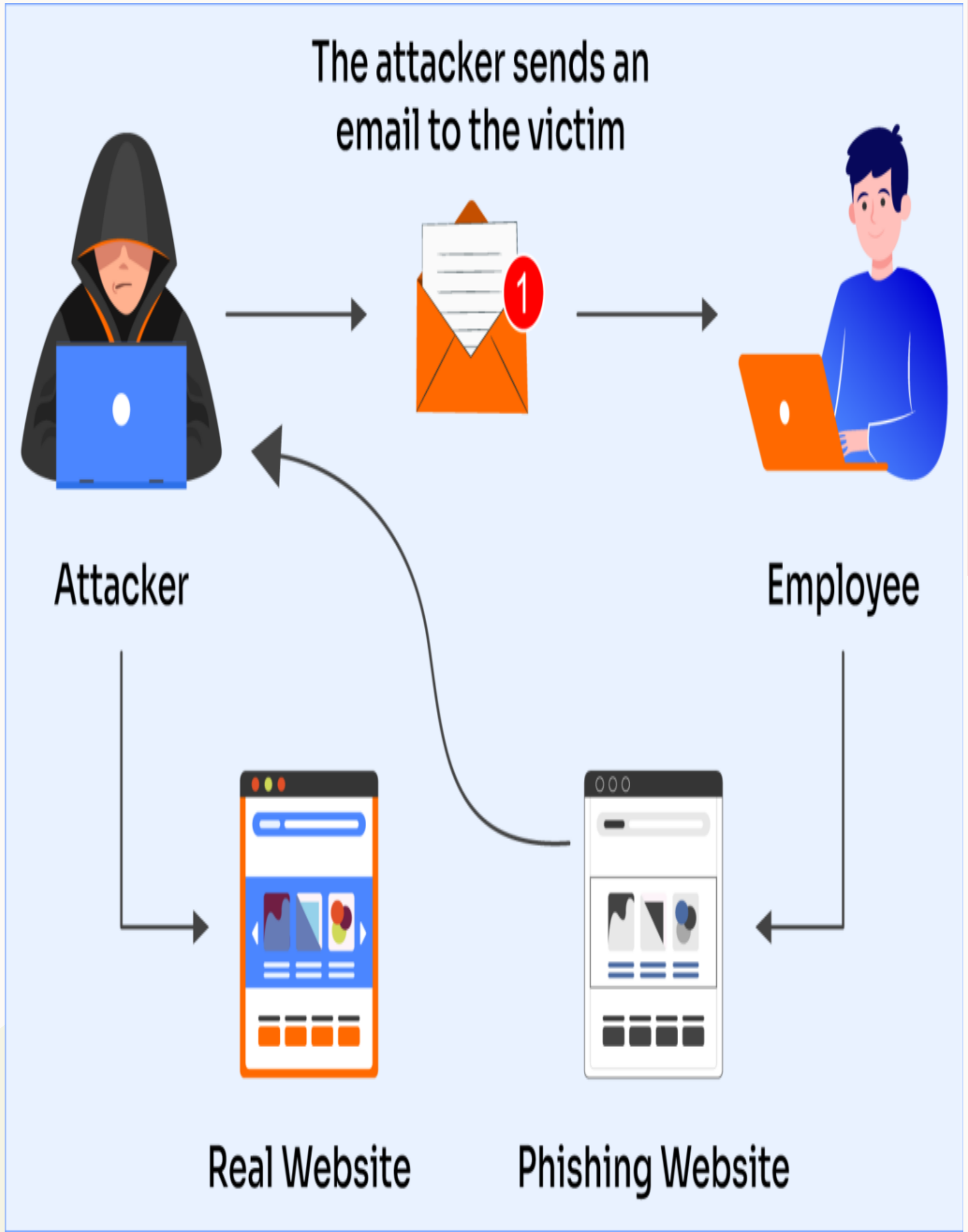
5.**Vishing**: Phishing conducted over the phone, often impersonating a bank or government official.

6.**Pharming**: Redirecting users from legitimate websites to fraudulent ones by exploiting vulnerabilities in domain name system (DNS) servers or browser settings.

HOW PHISHING EMAILS WORK

>Content:

- **Fake Sender Addresses:** Attackers often spoof the “From” address to make the email appear legitimate (e.g., “support@yourbank.com”).
- **Urgent Requests:** Phishing emails often create a sense of urgency, such as "Your account has been compromised. Act now!"
- **Suspicious Links:** They may include links to fake websites that look almost identical to real websites.
- **Attachments:** The email might contain malicious attachments (e.g., .exe, .zip) designed to install malware on your device.
- **Generic Greetings:** Phishing emails often use generic greetings such as "Dear Customer" instead of using your name



HOW TO RECOGNIZE PHISHING EMAILS

>**Content**:

1. **Check the sender’s email address**: Carefully inspect the sender’s address for discrepancies (e.g., support@banking-secure.com instead of support@bank.com).
2. **Look for typos or grammatical errors**: Legitimate organizations usually proofread their emails.
3. **Hover over links**: Hover your mouse over links to see the actual URL. Be wary if the URL is misspelled or looks unusual.
4. **Verify urgent r** Do not click on links or provide personal information in response to urgent, unsolicited requests.
5. **Avoid opening attachments**: Don’t open unexpected email attachments, especially if they come from unknown senders.

HOW TO RECOGNIZE PHISHING WEBSITES

>Content:

1. **Check the URL**: Ensure the website uses HTTPS (indicated by a padlock icon in the browser address bar) and that the domain is legitimate (e.g., www.amazon.com vs. www.amaz0n.com).
2. **Look for mismatched logos or design**: Phishing websites may have incorrect logos or formatting errors.
3. **Check for spelling errors**: Misspellings of the website name or content are a common red flag.
4. **Use Website Checkers**: Tools like Google Safe Browsing can tell you whether a website is known to be dangerous.

HOW TO RECOGNIZE SOCIAL ENGINEERING TACTICS

>**Content**:

1. **Pretexting**: Attackers create a fabricated scenario to obtain sensitive information from the victim (e.g., pretending to be a technical support agent).
2. **Baiting**: Attackers offer something enticing to get you to reveal sensitive information (e.g., offering free downloads in exchange for login details).
3. **Tailgating**: In a physical environment, attackers may follow authorized personnel into restricted areas, often using social manipulation.
4. **Impersonation**: Attackers may impersonate a trusted person or authority figure to convince you to divulge information.

REAL-WORLD PHISHING EXAMPLE

>Content:

Example 1: Show a screenshot of a phishing email (with personal information redacted). Walk through the signs: suspicious sender, mismatched URLs, and sense of urgency.

Example 2: A phishing website example showing how the URL and layout mimic a legitimate website.

HOW TO PROTECT YOURSELF

>**Content**:

1. **Don’t click on suspicious links**: Always verify links before clicking, especially in unsolicited emails.
2. **Verify via official channels**: If you receive a suspicious email or call, contact the organization directly using verified contact details.
3. **Enable two-factor authentication** (**2FA**): This adds an extra layer of protection to your accounts, even if your credentials are compromised.
4. **Update passwords regularly**: Use strong, unique passwords for each service, and change them periodically.
5. **Install security software**: Use antivirus and anti-malware programs that can detect phishing attempts and block harmful websites.

STEPS TO TAKE IF YOU FALL FOR A PHISHING ATTACK

>**Content:**

1.**Change your password :** immediately on any affected accounts.

2.**Contact your bank or service provider :** if you have shared sensitive financial information.

3.**Report the phishing attempt :** to the organization or service impersonated in the attack.

4.**Run a security scan** : to detect malware or other harmful software on your device.

5.**Notify your IT department or cybersecurity team** : to investigate and mitigate any risks.

KEY TAKEAWAYS

>Content

1. Phishing is a significant threat to personal and organizational security.
2. Recognizing phishing emails, websites, and social engineering tactics can prevent data loss.
3. Always verify requests, avoid clicking on suspicious links, and use security best practices like 2FA.
4. Stay cautious and report suspicious activity immediately.

THANK YOU.............