

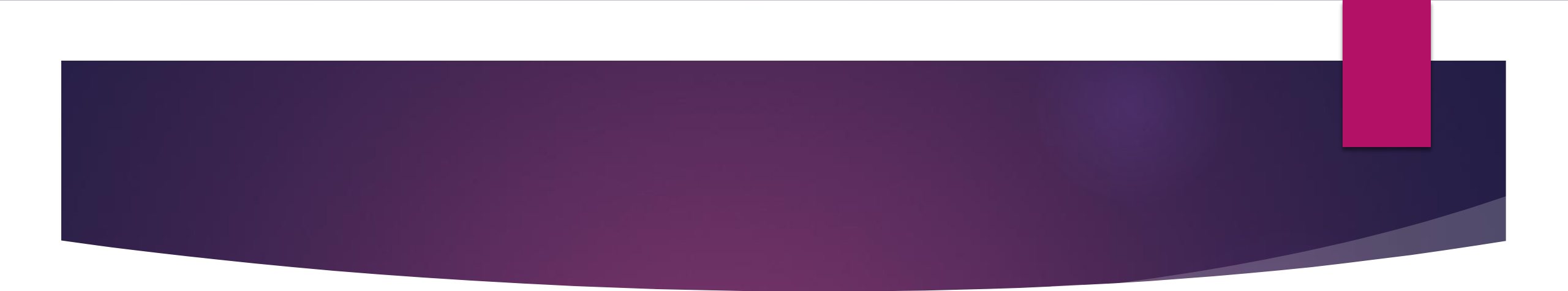
# Phishing Awareness: Training & Recognizing

# What is Phishing?

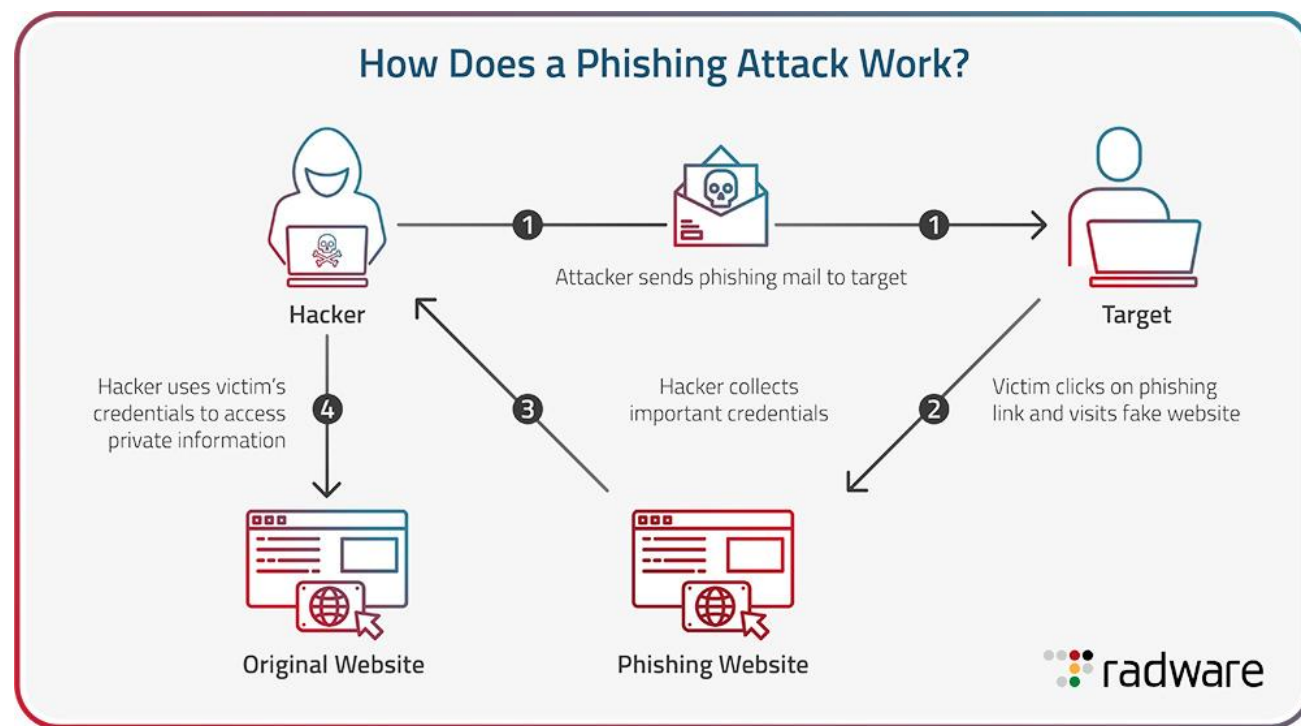
- ▶ Phishing attacks are one of the most common and effective cyber threats used by attackers to steal sensitive information such as usernames, passwords, and financial details.
- ▶ Phishing is a type of social engineering attack where cybercriminals trick individuals into revealing confidential information. These attacks are typically conducted through emails, fake websites, text messages or phone calls

# Types of Phishing Attacks



- 
- ▶ **Email Phishing:** Fraudulent emails designed to appear as if they come from trusted sources, often containing malicious links or attachments.
  - ▶ **Spear Phishing:** Targeted phishing attacks aimed at specific individuals or organizations using personalized information to increase credibility.
  - ▶ **Clone Phishing:** Attackers replicate legitimate emails but replace links or attachments with malicious versions..
  - ▶ **Smishing:** Phishing attempts that are carried out via **SMS** or Messaging apps.
  - ▶ **Vishing:** Voice phishing, where attackers use phone calls to manipulate victims into providing sensitive information.

# How Phishing works?



# Recognizing Phishing Attempts

## 1. Suspicious Email Addresses and Domains:

- ▶ Attackers often use email addresses that closely resemble legitimate ones but may have slight misspellings.
- ▶ Hover over links in emails to check their actual destination before clicking.

## 2. Urgent or Threatening Language:

- ▶ Phishing emails often create a sense of urgency, claiming that your account will be suspended or you must act immediately.

## 3. Generic Greetings:

- ▶ Attackers often use non-personalized greetings like "Dear Customer" instead of addressing you by name.



#### **4. Requests for Personal or Financial Information:**

- ▶ Legitimate companies rarely request sensitive information via email or text.

#### **5. Verify HTTPS encryption:**

- ▶ Look for Padlock symbol.

# How to Avoid Phishing Attacks

## **1. Verify Email Sources:**

- ▶ Contact the sender through official channels if you receive a suspicious email.

## **2. Use Multi-Factor Authentication (MFA):**

- ▶ This adds an extra layer of security, making it harder for attackers to access your accounts.

## **3. Check Website URLs:**

- ▶ Ensure websites use "https" and look for security certificates before entering sensitive information.

## **4. Keep Software and Security Tools Updated:**

- ▶ Regular updates help protect against known vulnerabilities



# Conclusion

- ▶ Phishing attacks continue to be a significant cybersecurity threat, that exploits human trust and digital vulnerabilities. By staying informed, practicing good security habits, and using technological defenses, individuals and organizations can reduce the risk of falling prey to these attacks. Therefore Having Awareness and vigilance are key in avoiding phishing and ensuring Online safety.



**THANK YOU!**