PHISHING AWARENESS TRAINING

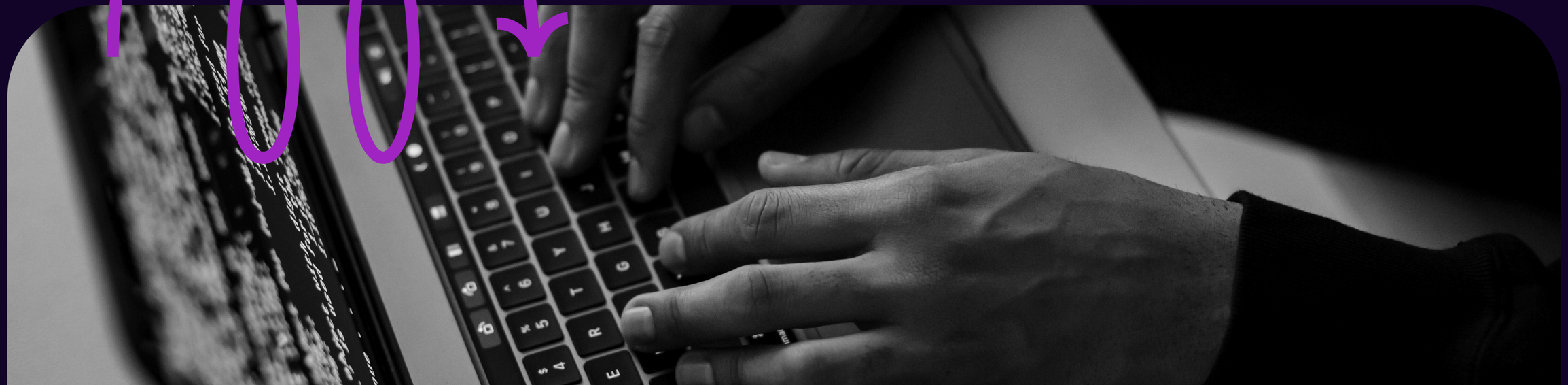
Recognize and Avoid Phishing Attacks

What is Phishing?

Phishing is a cyber-attack where attackers attempt to deceive individuals into providing sensitive information or installing malware by pretending to be a trustworthy entity.

Why is Phishing a Threat?

Phishing is one of the most common forms of cyber-attack. It can lead to significant financial loss, identity theft, and damage to personal and organizational reputations.



Types of Phishing Attacks

1. **Email Phishing:**
   Attackers send fake emails posing as trusted sources to steal credentials or install malware.

2. **Spear Phishing:**
   A customized phishing attack targeting a specific individual or organization using information about the target to make the attack more convincing.

3. **Whaling:**
   Spear phishing targeting high-profile individuals like executives.

4

Smishing:
Phishing via SMS with malicious links or info requests

5

Vishing:
Phishing over the phone, impersonating organizations to steal information.

6

Pharming:
Redirecting users to fake websites via DNS manipulation.

Recognizing Phishing Attempts

1

Unsolicited requests for personal information

2

Urgent or threatening language

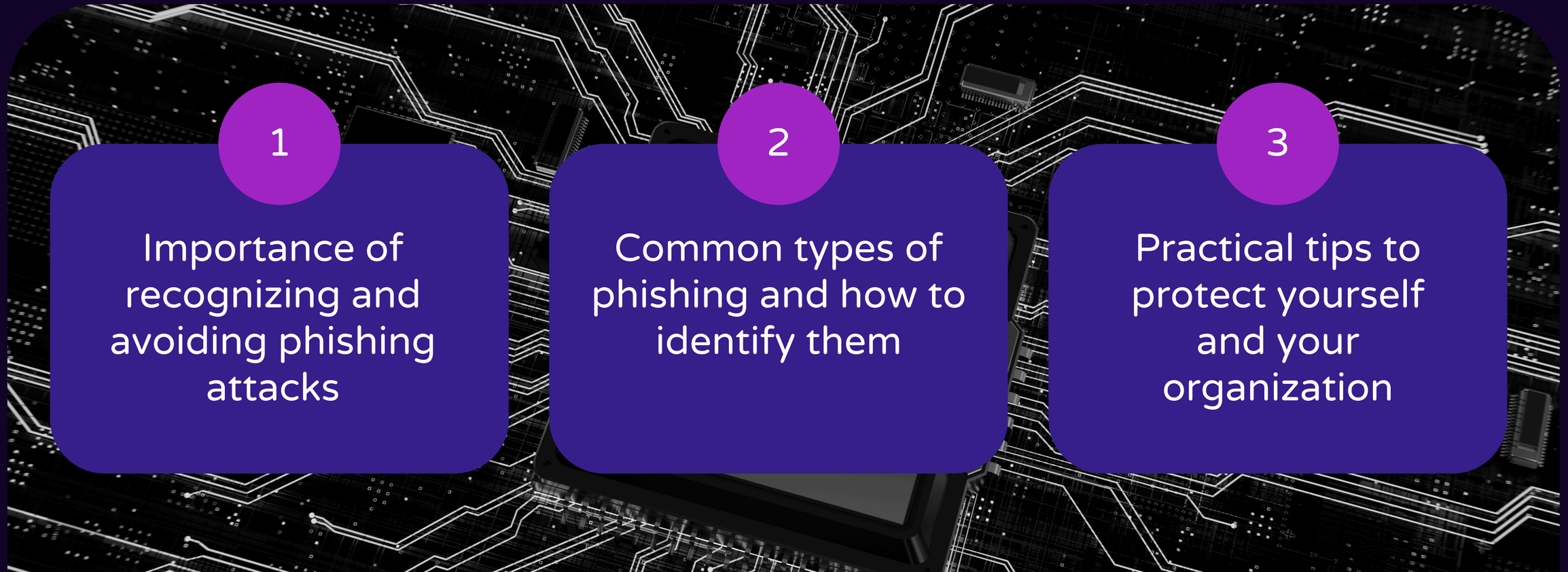
3

Suspicious links or attachments

Tips to Avoid Phishing Attacks

- Be cautious of unexpected requests for sensitive information.
- Use Strong Security Practices
- Look for spelling and grammatical errors in emails or websites.
- Verify Sources

Recap of Key Points



1. Importance of recognizing and avoiding phishing attacks
2. Common types of phishing and how to identify them
3. Practical tips to protect yourself and your organization

THANK YOU!