# Phishing Awareness

Protecting Yourself
and Your Organization

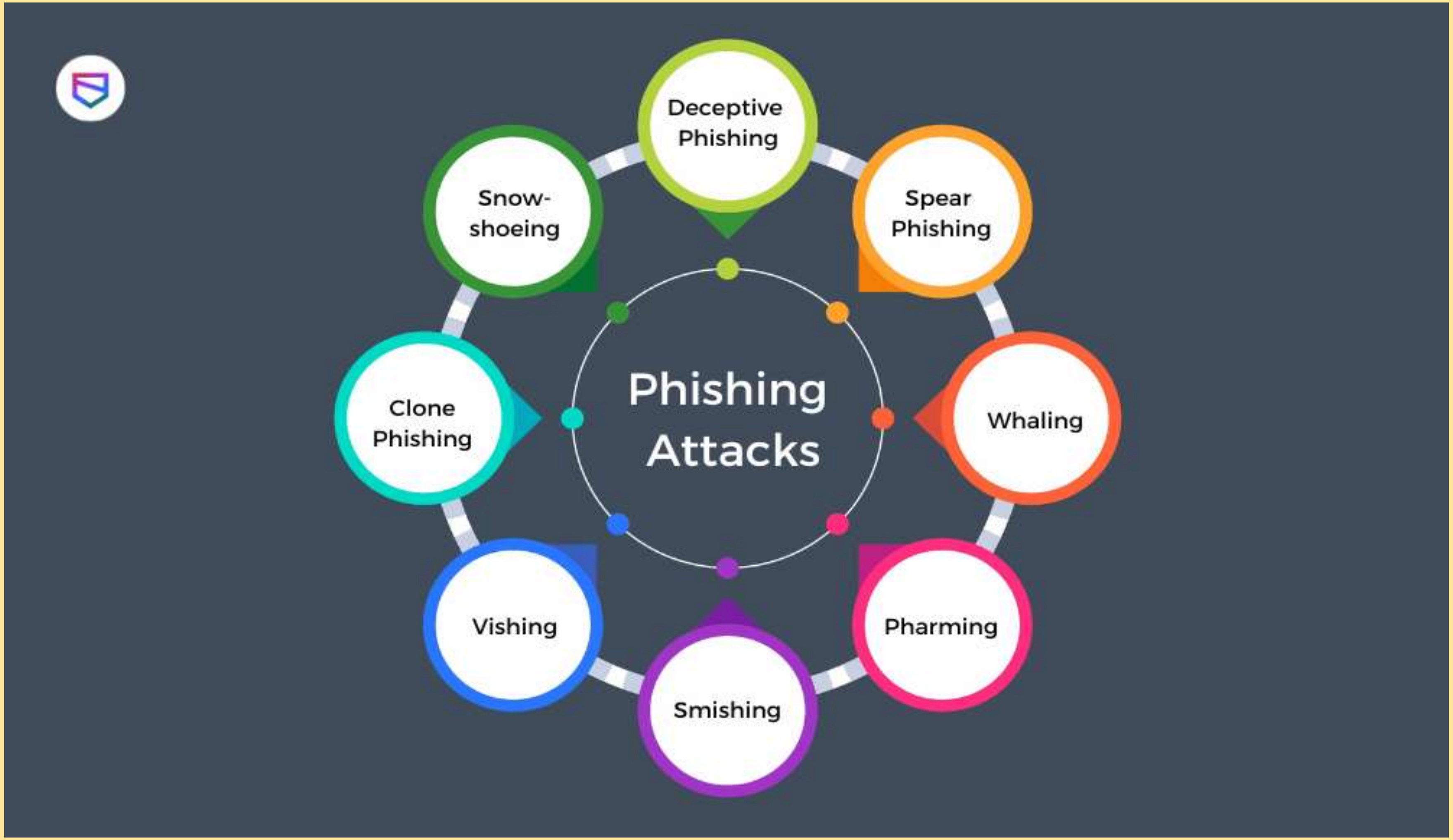
# Introduction to Phishing

- **Definition**: Phishing is a cyberattack that uses disguised emails or websites to steal sensitive information.

- **Image**: Example of a phishing email

- **Importance**: Understanding phishing is crucial to protecting personal and organizational data.

# Types of Phishing Attacks



# Anatomy of a Phishing Attack

Anatomy of a Phishing Attack
The Bait
The Hook
The Line
The Sinker

- Attack Vector: How the phishing message reaches the victim.

- Hook: The lure used to trick the victim (e.g., urgent request, attractive offer).

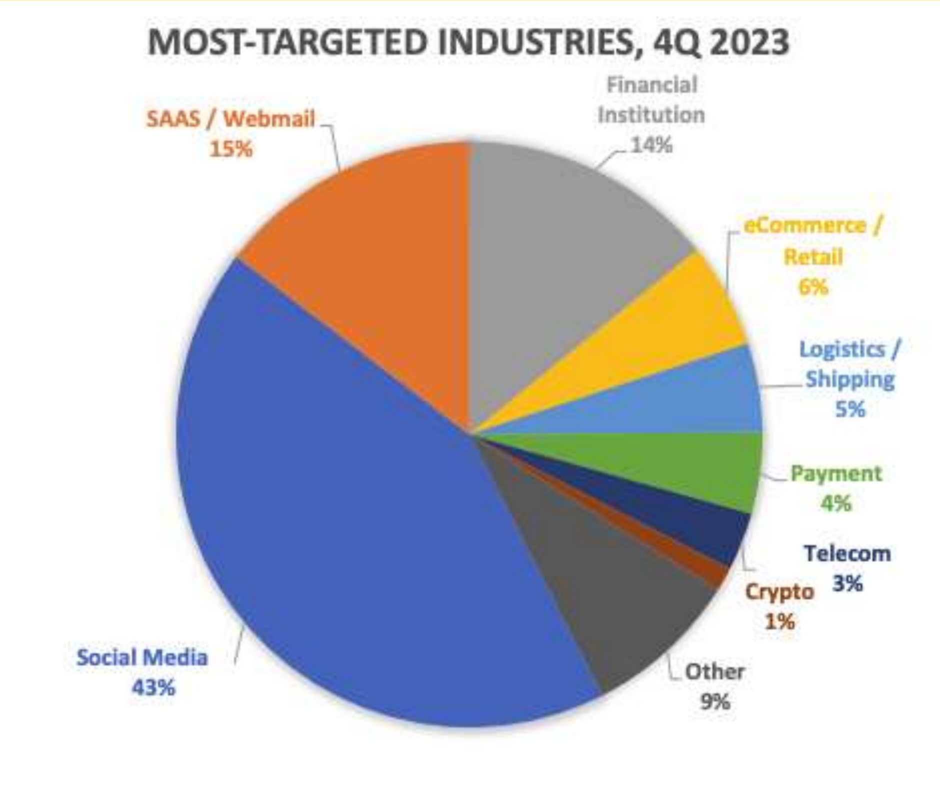
- Line: The method used to capture the victim's information (e.g., fake website, malicious attachment).

- Sinker: The execution of the attack (e.g., stealing data, installing malware).

# Identifying Phishing Emails

- Check the sender's email address.
- Look for generic greetings and poor grammar.
- Be wary of urgent or threatening language.
- Hover over links to see the actual URL.

# Impact of Phishing Attacks



- •Data Breaches: Loss of sensitive information.
- •Financial Loss: Direct theft or fraud.
- •Reputational Damage: Loss of trust from customers and partners.
- •Legal Repercussions: Compliance issues and fines.

# How to Protect Yourself

- Use strong, unique passwords.
- Enable multi-factor authentication (MFA).
- Regularly update software and systems.
- Be cautious with unsolicited emails and messages.

# What to Do if You’re Targeted

- Do not click on suspicious links or attachments.
- Report the phishing attempt to your IT department.
- Change your passwords immediately.
- Monitor your accounts for suspicious activity.

# Conclusion and Questions

# THANK YOU