# Phishing Awareness Guide

*Protect Yourself from Online Scams*

Marios Grivas Offensive Security Practicioner

## *What Is Phishing?*

Phishing is a type of cyberattack in which attackers disguise themselves as trustworthy entities—such as banks, service providers, or coworkers—to trick individuals into giving away **sensitive information** like **passwords**, **credit card numbers**, or **personal data**.

Phishing is most commonly delivered via **email**, **SMS**, or **fake websites that mimic legitimate ones**.

## *Common Targets:*

Small businesses and freelancers

- E-commerce store owners
- Anyone using email, banking apps, or social media

## *Common Phishing Attack Techniques:*

- **Email Phishing**
  Attackers send **fake emails** that appear to come from trusted organizations. These emails often **contain urgent language** (“Your account will be closed”) and **link to fraudulent websites**.
- **Spear Phishing**
  Targeted phishing that is **customized using publicly available information** (LinkedIn, company websites, etc.). These messages may **reference your actual coworkers, projects, or habits**.

- **Smishing**
  Phishing via **SMS text messages**. Often disguised as **messages from delivery companies or banks** asking you to click a link.
- **Vishing**
  Phishing via **voice calls**. The attacker **impersonates technical support, your bank, or government officials** to manipulate you into giving up private information.
- **Clone Phishing**
  A legitimate email is **duplicated**, and **its links or attachments are replaced with malicious ones**. It often looks like a **"resend"** or **"follow-up."**

*How to Recognize Phishing:*

- Misspelled URLs or email addresses.
- Urgent language or threats ("Act now!").
- Unexpected attachments or invoices.
- Generic greetings ("Dear customer").
- Requests for credentials or payments.

Tip! Hover over links to see where they really lead.

*How to Protect Yourself:*

- Never click links in suspicious emails or texts.
- Always verify the sender's email address.
- Use two-factor authentication (2FA) wherever possible.
- Keep your software and antivirus updated.
- Report suspicious emails to your organization or email provider.

*What to Do If You Suspect Phishing:*

- Do NOT click any links or download attachments.
- Forward the message to your company's IT/security team or to phishing-report@yourdomain.com.
- Delete the message from your inbox and trash.
- If you clicked, change your passwords immediately and monitor your accounts for unusual activity.