



# PHISING AWARENESS TRAINING

BY  
H A R I H A R A N R



Phishing is a common attack method that can lead to identity theft, financial loss, or corporate data breaches.

# TYPES OF PHISHING ATTACKS

**Email Phishing:** Fake emails disguised as coming from legitimate organizations.

**Spear Phishing:** Targeted phishing aimed at specific individuals.

**Smishing:** Phishing attacks through SMS messages.

**Vishing:** Phishing via phone calls.

**Clone Phishing:** Creating a nearly identical version of a legitimate email to trick the recipient.





# ANATOMY OF A PHISHING EMAIL

Sender's Address: Fake or similar-looking domain names.

Urgent Language: "Immediate Action Required!" or "Account Suspended."

Suspicious Links or Attachments: Links that do not match the visible text.

Grammatical Errors: Poor grammar and spelling mistakes.

Request for Personal Information: Legitimate companies will not ask for sensitive information through email.





## HOW TO RECOGNIZE PHISHING WEBSITES

**URL Inspection:** Always check for HTTPS and verify the domain name carefully.

**Poor Design:** Bad grammar, incorrect formatting, or strange logos.

**Unexpected Pop-Ups:** Requests for personal information in pop-up windows.

**Suspicious Offers:** Deals or promotions that seem too good to be true

## SOCIAL ENGINEERING TACTICS

**Impersonation:** Attackers posing as coworkers or authorities.

**Trust Exploitation:** Playing on emotions like fear, curiosity, or urgency.

**Spoofing:** Creating fake caller IDs or websites to trick victims.





## REAL-WORLD EXAMPLES

Provide screenshots of common phishing emails and discuss how they appear convincing.

Talk about recent phishing incidents that have affected businesses or individuals.

## BEST PRACTICES TO AVOID PHISHING

**Think Before Clicking:** Don't click on links or open attachments unless you're certain of their source.

**Verify the Source:** Contact the sender directly using a trusted method if unsure.

**Enable Multi-Factor Authentication (MFA):** Adds a layer of security.

**Keep Software Updated:** Stay protected with the latest security patches.

# WHAT TO DO IF YOU SUSPECT PHISHING

Don't Interact: Do not reply, click on links, or download attachments.

Report to IT: Notify your IT department immediately.

Change Passwords: Update your passwords if you clicked on a link or submitted information.







pngtree.com

## SUMMARY

Be vigilant against phishing attacks.

Understand common tactics and how to recognize phishing emails and websites.

Report any suspicious activity immediately.

## RESOURCES AND FURTHER LEARNING

Provide links to trusted websites like Anti-Phishing Working Group or US-CERT.

Mention company-specific security training materials.



# THE CONCLUSION

Thank everyone for their participation.

This structure can be used for both a presentation or an online module. You can make it interactive by adding quizzes, real-world examples, and animations to keep the audience engaged.





# THANK YOU