


Introduction to Phishing Attacks

Phishing attacks are malicious attempts to deceive individuals into disclosing sensitive information, such as usernames, passwords, and credit card details. These attacks are commonly carried out through email, fraudulent websites, or other forms of online communication.

 by Minor Project



What is Phishing?

1

Deceptive Strategy

Phishing involves impersonating a trustworthy entity to trick individuals into divulging personal information.

2

Social Engineering

It leverages psychological manipulation to elicit the desired response from the target to gain unauthorized access.

Common Types of Phishing Attacks

Email Phishing

Attackers use fraudulent emails to extract sensitive information from unsuspecting recipients.



SMS Phishing

Perpetrators send deceptive text messages to deceive individuals into sharing personal details.



Vishing

Phishing carried out through voice calls, attempting to extract sensitive information over the phone.





!! PHISHING EMAIL !!

Recognizing Phishing Emails

1 Suspicious Sender

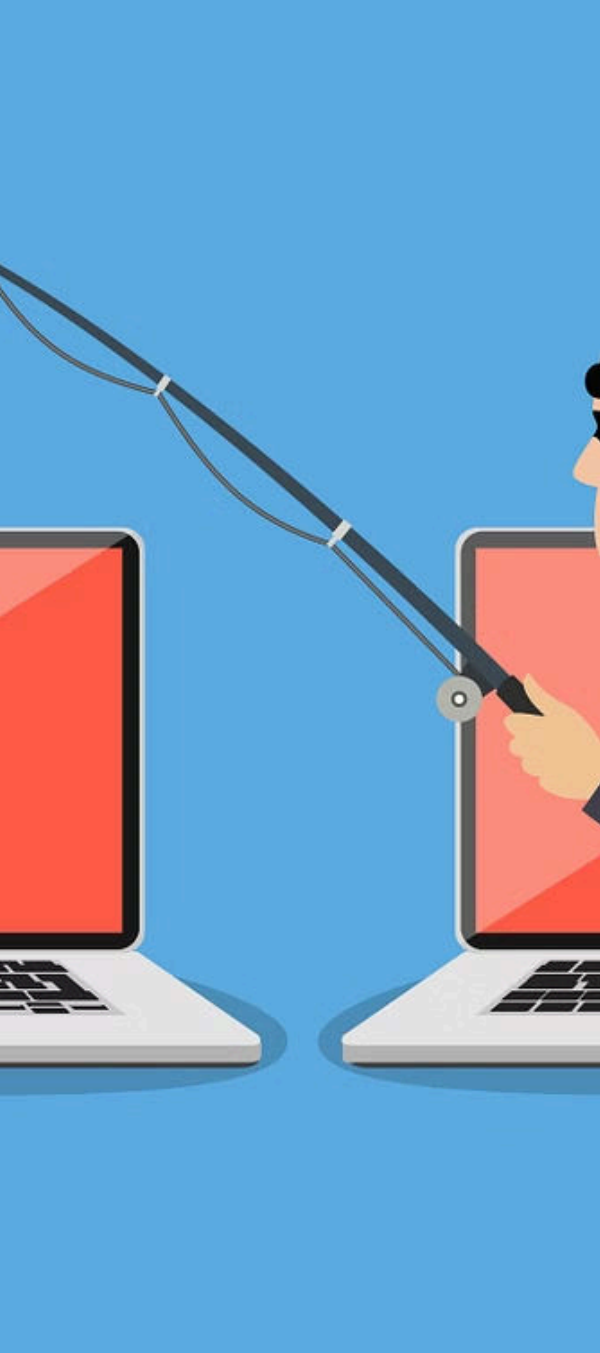
Check the sender's email address for misspellings or slight variations from legitimate ones.

2 Urgent Requests

Beware of urgent requests for personal or financial information, especially with warning of dire consequences.

3 Unsolicited Attachments

Avoid opening attachments from unknown senders, as they may contain malware or ransomware.



Identifying Phishing Websites

1 Verify URL

Inspect the URL for misspellings, extra characters, or variations that deviate from the legitimate website's address.

2 Lack of Security Badges

Avoid websites lacking security badges, SSL encryption, and other trust indicators.

3 Unsolicited Pop-Ups

Avoid clicking on pop-ups asking for personal or sensitive information, especially if unsolicited.

Avoiding Phishing Scams



Update Software

Regularly update operating systems, browsers, and security software to patch vulnerabilities.



Enable Two-Factor Authentication

Add an extra layer of security by implementing two-factor authentication for accounts.



Monitor Financial Statements

Regularly review bank and credit card statements for unauthorized transactions.



Stay Informed

Stay updated on common phishing trends and techniques to enhance awareness.



Reporting Phishing Attempts

1

Internal Reporting

Establish clear procedures for employees to report suspected phishing attempts within the organization.

2

External Reporting

Encourage the reporting of phishing emails or websites to relevant authorities or institutions.



Best Practices for Protecting Against Phishing Attacks

1

User Education

Conduct regular training sessions to educate individuals on recognizing and mitigating phishing threats.

2

Email Filters

Implement robust email filtering to minimize the inflow of phishing emails into inboxes.

3

Incident Response Plan

Develop and maintain a comprehensive incident response plan to handle suspected phishing incidents.