WELCOME

TO THIS PRESNTATION

CODE ALPHA

NAME:-DHARMENDRA KUMAR

STUDENT ID: CA/AG3/31277

PHISHING AWARNESS TRANING

INTRODUCTION

- Phishing is a type of cyber attack.
- Involves tricking individuals int revealing sensitive information.
- Importance of Phishing Awarness.

TYPES OF PHISHING ATTACKS

- Social Engineering
- Website Phishing
- Email Phishing

TYPES OF PHISHING ATTACK

Social Engineering

- Manipulating individuals to divulge confidential information.
- Social engineering is the art of convincing people to reveal confidential information
- Social engineering depend upon on the fact people are unware of the valuable information to which they have access and are careless about protecting it
- Example :- Impersonation, emotional manipulation

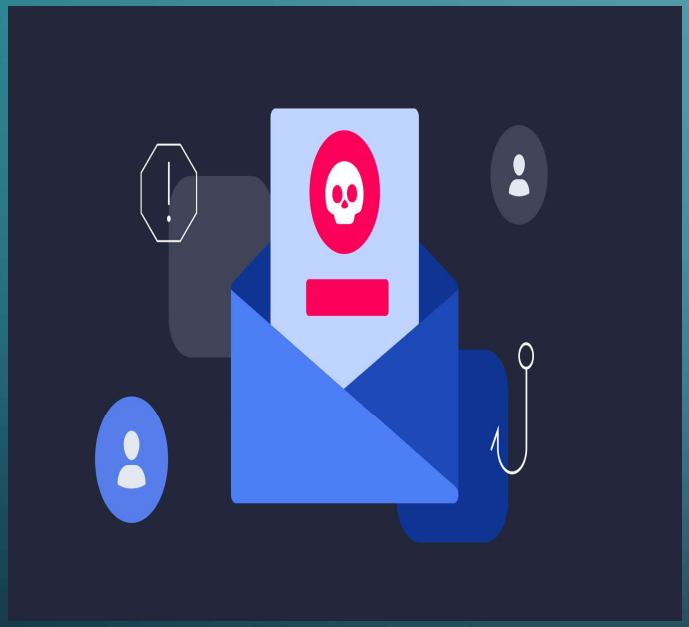
Website Phishing

- Fraudulent websites imitating legitimate ones.
- A phishing website (spoofed website) is a common deception tactic threat actors utilize to steal real login credentials to legitimate websites. This operation, commonly called credential theft, involves sending victims an email that spoofs a trusted brand, trying to trick them into clicking on a malicious link.
- Example :- Fake login pages, malicious websites

Email Phishing

- Deceptive emails to extract information.
- Phishing is an attempt to steal personal information or break in to online accounts using deceptive emails, messages, ads, or sites that look similar to sites you already us.
- For example, a phishing email might look like it's from your bank and request private information about your bank account.

COMMON CHARACTERISTICS OF PHISHING ATTEMPTS



- Urgency: Creating a sense of immediate action.
- Unexpected Emails: Receiving unsolicited emails.
- Unexpected Emails: Receiving unsolicited emails.
- Requests for Personal Information: Be cautious.

Preventive Measures

•For Individuals

- **Verify Senders:** Double-check the sender's email address.
- **Hover Over Links:** Before clicking, see where the link actually leads.
- **Use Two-Factor Authentication (2FA):** Add an extra layer of security.
- **Keep Software Updated:** Regular updates reduce vulnerabilities.

•For Organizations

- **Employee Training:** Regular phishing simulation exercises.
- **Email Filtering Tools:** Deploy spam filters and antivirus software.
- **Incident Response Plan:** Have a plan in place for phishing attacks.

CONCLUSION

- **Key Takeaways**
  - Importance of vigilance in identifying phishing attempts.
  - Continuous education and awareness are crucial.
- **Q&A:**
  - Open the floor for any questions from the audience.

Thank You

I appreciate your time and active participation in today's presentation on safeguarding against phishing attacks.