- Phishing is one of the most prevalent cyber threats targeting individuals and organizations worldwide.
- This training module analyzes attack techniques, psychological manipulation methods, real-world case study analysis, and prevention strategies to strengthen digital security posture.

PHISHING AWARENESS & SOCIAL ENGINEERING ANALYSIS

- Phishing is a social engineering attack designed to manipulate victims into disclosing sensitive information.

- Login credentials and passwords

- One-Time Passwords (OTP)

- Banking and financial data

- Personal identification information

- Unlike traditional hacking, phishing exploits human trust instead of software vulnerabilities.

WHAT IS PHISHING? (TECHNICAL PERSPECTIVE)

- Email Phishing – Mass impersonation campaigns.
- Spear Phishing – Highly targeted attacks.
- Whaling – Executive-level targeting.
- Smishing – SMS-based phishing.
- Vishing – Voice call scams.
- Social Media Phishing – Fake brand collaborations.
- Clone Phishing – Replica of legitimate emails with malicious links.

TYPES OF PHISHING ATTACKS

PSYCHOLOGICAL MANIPULATION IN PHISHING

- Phishing exploits emotional triggers:

- Urgency – 'Act immediately.'
- Fear – 'Your account is compromised.'
- Greed – 'Earn quick money.'
- Authority – Impersonating officials.
- Trust – Mimicking legitimate brands.

- Humans react emotionally before logically verifying authenticity.

- A normal Instagram user received a message from a fake advertising agency offering paid tasks.
- The attacker built trust using professional language and reward promises.
- Victim was instructed to add attacker’s email to account settings.
- Screenshot confirmation was requested.
- Within one minute, account was fully taken over.

CASE STUDY: INSTAGRAM ACCOUNT TAKEOVER

1. Reconnaissance – Target identification.
2. Initial contact with fake collaboration offer.
3. Trust building through conversation.
4. Privilege escalation by adding attacker email.
5. Password reset via new recovery email.
6. Account lockout and removal of original owner.

TECHNICAL BREAKDOWN OF THE ATTACK

INCIDENT RESPONSE & RECOVERY

- Immediate recovery actions:

- Used Instagram recovery process.
- Verified identity.
- Reset password.
- Enabled Two-Factor Authentication.
- Removed unauthorized email access.

- Rapid response prevented permanent account loss.

- Never modify recovery settings for unknown contacts.
- Enable Multi-Factor Authentication.
- Verify brand collaborations independently.
- Use strong, unique passwords.
- Implement SPF, DKIM, DMARC for email protection.
- Conduct regular security awareness training.

PREVENTION & ORGANIZATIONAL CONTROLS

1. Why did the Instagram attack succeed?
2. What action allowed attacker access?
3. What is strongest defense against phishing?

- Correct Answers: 1-Social Engineering, 2-Adding attacker email, 3-Awareness + MFA

KNOWLEDGE ASSESSMENT