Course Code	**:**	**MSEI-023**
Course Title	**:**	**Cyber Security**
Assignment Number	**:**	**BCA_NEW/BCAOL(V)023/Assign/2026-27**
Maximum Marks	**:**	**20**
Last Date of Submission	**:**	**31st October, 2026 (For July 2026 Session) (For latest updates, refer SED Notification On IGNOU's website)**

There are two questions in this assignment. Answer all the questions. You may use illustrations and diagrams to enhance your explanations.

Q1: All the security measures that the organization adopts go in vain when employees get "social engineered" by strangers. Do you agree with this statement and also suggest the measures. **(10 Marks)**

Q2: The Internet is not just a vast array of computers connected to each other. There are a host of networking devices like the router, which control the data traffic between and within networks. Explain Internet routing in detail? **(10 Marks)**

Q1: All the security measures that the organization adopts go in vain when employees get “social engineered” by strangers. Do you agree with this statement and also suggest the measures. (10 Marks)

Answer

I largely agree with the statement because an attacker can bypass expensive technical defences by persuading an employee to provide access. Firewalls, antivirus programs, encryption and access-control systems protect an organisation, but people use and administer these systems. If an employee reveals a password, approves a fraudulent login request or transfers confidential records, the attacker may enter through an apparently authorised route. However, it is not correct to say that all security measures necessarily become useless. Well-designed controls can still prevent, limit or detect the damage. The real lesson is that people, processes and technology must work together.

How social engineering creates a security risk

Social engineering means manipulating a person into performing an action or disclosing information that benefits an attacker. Criminals exploit trust, fear, urgency, curiosity, helpfulness or the apparent authority of a senior officer. They may first collect names and job roles from public websites, then approach their target through a convincing message or telephone call. Common forms include phishing emails, fraudulent text messages (smishing), deceptive calls (vishing), impersonation of IT support, baiting with free downloads, and physical tailgating into restricted premises.

For example, a caller may pretend to work for the IT help desk and tell an employee that a security issue requires immediate verification of a one-time passcode. If the employee shares the code, the criminal might sign in using a stolen password. Similarly, a fake message from a manager could cause an accounts employee to pay a false invoice. These incidents can lead to data theft, malware installation, financial loss, business interruption and damage to customer confidence. They show why a security policy on paper is not sufficient if employees cannot recognise suspicious requests.

Measures to prevent and control social engineering

Practical security education: Train all employees during induction and at regular intervals. Use realistic examples of suspicious links, fake login pages, QR-code scams and urgent payment requests. Short phishing simulations followed by constructive feedback can help employees practise recognition rather than merely memorise rules.