Cybersecurity Scenarios and Solutions

Phishing Email Attack

Situation: A company employee receives an email from 'IT Support' stating that their password is expiring and that they must click a link to update it. The email contains an urgent request, a suspicious link, and a request for login credentials.

Solution:

- Verify the Sender - Check the sender's email address for discrepancies.
- Hover Over Links - Do not click; hover over the link to inspect the URL.
- Report to IT - Forward the email to the IT security team for verification.
- Enable Multi-Factor Authentication (MFA) - Even if credentials are stolen, MFA prevents unauthorized access.
- Educate Employees - Regular cybersecurity awareness training reduces phishing success rates.

Ransomware Infection

Situation: An employee unknowingly downloads a file from an unverified email attachment. Within minutes, all files on the company's system become encrypted, and a message appears demanding a ransom in Bitcoin.

Solution:

- Isolate Infected Systems - Immediately disconnect affected computers from the network to prevent spread.
- Restore from Backup - If recent, clean backups exist, use them instead of paying ransom.
- Report to Authorities - Involve cybersecurity professionals and law enforcement.
- Educate Employees - Train employees to avoid suspicious downloads and attachments.
- Implement Endpoint Protection - Use antivirus and intrusion detection software to monitor file behaviors.

Insider Threat

Situation: A disgruntled employee, with access to sensitive company financial records, decides to copy and leak confidential files before quitting their job.

Solution:

- Implement Access Controls - Follow the principle of least privilege (employees access only what they need).
- Monitor User Activity - Use security monitoring tools to track unusual behavior.
- Enforce Data Loss Prevention (DLP) Policies - Restrict unauthorized data transfers via USB or email.
- Disable Access Immediately - When an employee leaves, revoke access credentials immediately.
- Conduct Exit Interviews - Assess employee concerns to prevent insider threats.

Public Wi-Fi Attack (Man-in-the-Middle)

Situation: A remote worker connects to free public Wi-Fi at a coffee shop. A hacker in the same network uses a Man-in-the-Middle (MITM) attack to intercept login credentials when the worker accesses their corporate email.

Solution:

- Use a VPN - Always use a Virtual Private Network (VPN) when on public Wi-Fi.
- Disable Auto-Connect - Prevent devices from automatically joining unknown Wi-Fi networks.
- Use HTTPS Websites - Ensure all web traffic is encrypted by checking for 'https://' in the URL.
- Avoid Logging into Sensitive Accounts - Do not enter banking credentials or company logins on public networks.
- Enable Multi-Factor Authentication (MFA) - Protects against credential theft.

CEO Fraud (Business Email Compromise)

Situation: A finance employee receives an email appearing to be from the CEO requesting an urgent wire transfer of EUR50,000 to a 'vendor.' The email is well-crafted, impersonates the CEO, and pressures the employee to act fast.

Solution:

- Verify Requests via Phone - Call the CEO directly to confirm the request.
- Use Email Filtering - Enable domain authentication (DMARC, SPF, DKIM) to detect spoofed emails.
- Implement Approval Workflows - Require dual approval for financial transactions above a certain amount.
- Train Employees on Social Engineering - Awareness training helps employees recognize fraud attempts.
- Report Fraudulent Attempts - Notify IT and law enforcement if fraud is suspected.