Scenario 1: CEO Impersonation

The hacker conducts extensive research on the company and its key executives. They then pose as the CEO and contact an employee in the finance department, urgently requesting a wire transfer to a specific account. The employee, believing it's a genuine request from the CEO, bypasses security protocols and transfers the funds, unknowingly falling victim to the hacker's social engineering attack.

Scenario 2: Help Desk Manipulation

The hacker calls the company's help desk, pretending to be an employee experiencing technical difficulties. They provide enough personal information to convince the help desk representative of their identity and claim they need immediate access to a sensitive system. The representative, thinking they are assisting a legitimate employee, bypasses security controls and grants the hacker unauthorized access.

Scenario 3: Tailgating

The hacker observes the company's employees entering the premises and takes advantage of a busy moment to slip through the security checkpoint without identification. By tailgating behind an authorized employee, the hacker gains physical access to restricted areas or computer systems, bypassing the company's security measures.

Scenario 4: Vendor Exploitation

The hacker poses as a vendor representative and contacts an employee responsible for managing vendor relationships. They claim there is an urgent issue with a recent invoice and request the employee's login credentials to rectify the problem. Believing it's a legitimate request, the employee unknowingly provides the hacker with access to the company's systems, enabling them to bypass cybersecurity controls.

Scenario 5: Employee Training Scam

The hacker sends an email to all employees, disguising it as a mandatory security training exercise. The email contains a link to a fake training portal that requires employees to enter their login credentials. Unaware of the scam, employees willingly provide their credentials, allowing the hacker to bypass security controls and gain unauthorized access to sensitive data and systems.