**Assingment - 3**

**Step-1 Case Study Analysis:**

- **Email Spoofing:** The attackers spoofed the email address to make it appear as if it came from a legitimate source, the IT department.
- **Fake Website:** The email contains a link to a fake website that mimics the company's login page. Unsuspecting employees enter their credentials, which are then captured by the attackers.
- **Data Breach:** The attackers gain access to employee login credentials, potentially compromising sensitive company information.
- **Employee Training:** Conduct regular training sessions to educate employees about phishing techniques and how to identify suspicious emails.

**Step-2 Role play exercise:**

- You are a cybersecurity analyst at a large financial institution.
- I'll play the role of a malicious actor attempting to gain unauthorized access to sensitive information from your company's network through social engineering tactics.
- Your goal is to detect and respond appropriately to my attempts to manipulate you into divulging confidential information or performing unauthorized actions.
- Stay vigilant and trust your instincts. If something seems suspicious, it probably is.

**Step-3 phishing Email Analysis**

- **Urgency:** The email creates a sense of urgency by claiming that unauthorized access attempts have been detected and implying that immediate action is required to prevent further harm.
- **Fear:** By mentioning potential account suspension, the email instills fear in the recipient, making them more likely to act hastily without thoroughly verifying the request.
- **Spoofed Sender:** The sender's email address appears to be from the legitimate domain of the recipient's bank (yourbank.com), but it could be spoofed. Always verify email addresses by hovering over them or checking the sender's details.
- **Generic Greeting:** The email starts with a generic greeting ("Dear Valued Customer"), indicating that it's a mass email sent to many recipients rather than a personalized message.

**Step-4 Documenting the Exploit Process:**

- Certainly, documenting the exploit process is crucial for understanding how the attack occurred and implementing measures to prevent similar incidents in the future.
- Briefly describe the phishing attack, including the method used (email spoofing), the content of the phishing email, and the goal of the attacker (to steal login credentials).