Incident Response Playbook

Phishing/Spoofing

Phase 1: Preparation

Form an incident response team with professionals in communication, law, and information technology.

Develop a communication strategy that lists all relevant parties and gives their contact details.

Establish policies and processes for incident response.

Every employee should get regular security awareness training.

Phase 2: Detection and Analysis

Analyze log files for indications of a phishing or spoofing attack while looking out for strange behavior in network traffic.

Determine the attack's origin and the extent of the occurrence.

In order to prevent further damage, shut down or isolate the damaged account or system.

Gather and keep track of any relevant evidence.

Phase 3: Containment, Eradication, and Recovery

Disconnect the impacted system or disable the compromised account to contain the situation.

Remove the virus or phishing email and make sure the machine is secure before resuming normal operation.

In order to prevent such attacks in the future, restore any lost or compromised data and make sure that all systems and apps are updated.

Restore the system or account affected to its previous state.

Phase 4: Communication and Notification

Inform all the stakeholders about the situation, including staff members, clients, and partners.

Explain the occurrence and the actions being done to lessen the situation in a straightforward and succinct manner.

Offer support to impacted persons, such as credit monitoring or identity theft protection.

Phase 5: Post Incident Activity

Conduct a post-event evaluation to find areas where incident response rules and processes need to be improved.

Update the incident response playbook to include any new information.

Train staff members on security awareness in greater detail.

Monitor the afflicted system or keep an eye out for any indications of recurrence