**Incident Response Process**

**Scenario Details:**

**Phishing Attack**: An employee of the organization receives an email with the title "account verification" and the email contains a malicious link.

**Malicious Link:** The link leads to a malicious website that asks for "confirmation" for the user to enter their password.

**Impact:** The user unwittingly transmits his login information to malicious parties.

**1. Preparation (People, Process, Technology)**

* **People**:
  + **Employee Awareness**: Ensure employees have been trained to recognize phishing attempts, such as suspicious emails with generic subject lines (e.g., "account verification") or unfamiliar sender addresses.
  + **Incident Response Team**: Ensure roles are defined, and the team is trained to handle phishing incidents. Roles may include:
    - **Incident Response Manager**: Oversees the response process.
    - **Security Analysts**: Investigate the phishing email and its impact.
    - **IT Support**: Assist with isolating affected systems and users.
* **Process**:
  + **Phishing Incident Playbook**: Ensure the organization has a clear playbook detailing the steps to take when a phishing attempt occurs.
  + **Reporting Channel**: Employees should report suspicious emails immediately via a predefined channel (e.g., a dedicated email or a reporting tool).
* **Technology**:
  + **Email Filtering Tools**: Utilize spam filters and anti-phishing tools to catch and block phishing emails before they reach employees.
  + **EDR Tools**: Ensure Endpoint Detection and Response (EDR) systems are in place to monitor and detect suspicious activity following any phishing links clicked.

**2. Identification**

* **People**:
  + **Employee Reports the Email**: The employee identifies the suspicious email and reports it to the IT/security team. This is done through the company's designated phishing reporting tool or email address.
* **Process**:
  + **Initial Investigation**: The security team investigates the reported phishing email:
    - **Email Analysis**: Check the sender’s address and examine the email content. In this case, the subject "Account Verification" and the use of a malicious link are red flags.
    - **URL Check**: Analyze the URL provided in the email. Verify if it matches the legitimate domain, which it likely will not. Use online tools (e.g., URL scanners) to check the legitimacy of the link.
    - **Impact Assessment**: Check if the link was clicked by any other employees, and if passwords have been entered into the malicious site.
* **Technology**:
  + **ELK Stack**: Use **ELK Stack** (ElasticSearch, Logstash, Kibana) to search for logs related to the phishing email and track employee interactions with the malicious link.
  + **Web Filtering Logs**: Check web filtering logs for any traffic to the malicious website.

**3. Containment**

* **People**:
  + **Incident Response Team**: Once the phishing email and malicious link are confirmed, the security team takes immediate action.
* **Process**:
  + **Isolate the Affected Systems**: If an employee has clicked the link, immediately disconnect their system from the network to prevent further data exfiltration or malware installation.
  + **Alerting and Communication**: Notify other employees of the phishing attempt, and remind them not to click on suspicious links or enter credentials on any unfamiliar sites.
  + **Password Reset**: Instruct the employee to reset their passwords for all accounts, especially if they have entered their credentials on the malicious site.
* **Technology**:
  + **Email Blocking**: Use email security systems to block the malicious sender and prevent similar phishing emails from reaching others in the organization.
  + **Network Segmentation**: If necessary, segment the network to isolate affected systems and prevent lateral movement.

**4. Eradication**

* **People**:
  + **Security Analysts and IT Support**: Collaborate to clean up the system and remove any remnants of the attack.
* **Process**:
  + **Malware Scan**: Run a full malware scan on the affected system to detect any installed malware or keyloggers.
  + **Credential Review**: Check if the compromised credentials have been used on any other critical accounts. If necessary, reset those accounts as well.
  + **Patch Vulnerabilities**: If the phishing attack exploited any vulnerabilities (e.g., outdated software or a vulnerable browser plugin), ensure patches and updates are applied immediately.
* **Technology**:
  + **EDR Tools**: Use EDR to scan and remove any malicious artifacts that may have been downloaded to the affected device.
  + **Email Filtering Update**: Update email filters to detect and block similar phishing emails with new phishing tactics or email addresses.

**5. Recovery**

* **People**:
  + **Employee**: The affected employee must ensure that all accounts and devices are fully restored to a secure state, including password resets and re-enabling network access.
* **Process**:
  + **System Restoration**: Restore the affected systems from clean backups if necessary, ensuring that no traces of the attack remain.
  + **Monitoring**: Continuously monitor the affected system for signs of any recurring issues, including the appearance of additional phishing emails or further malicious activity.
  + **Reinforce Security**: Implement additional security measures such as multi-factor authentication (MFA) for critical accounts and email verification.
* **Technology**:
  + **Restore from Backup**: Ensure that systems are restored from backups that have not been compromised.
  + **Email System Review**: Confirm that the email filtering system is effectively catching similar phishing attempts in the future.
  + **ELK Stack**: Use **ELK Stack** to monitor traffic from affected systems and ensure no malicious activity continues.

**6. Lessons Learned**

* **People**:
  + **Incident Response Team**: The team conducts a post-incident review with key stakeholders (management, IT, HR, security).
* **Process**:
  + **Post-Incident Analysis**: Analyze the steps taken during the response process. Did the team identify the phishing attempt in a timely manner? Were any delays caused by ineffective communication or lack of awareness?
  + **Process Improvement**: Revise and improve phishing response protocols based on lessons learned. This could involve adjusting email filtering, employee training, or response timelines.
  + **Reporting and Documentation**: Create a detailed report documenting the phishing attack, including what happened, how it was detected, the actions taken, and the recovery steps. This document will serve as a reference for future incidents.
* **Technology**:
  + **Improved Email Filtering**: Update email filtering systems to recognize and block similar phishing tactics used in this attack.
  + **Phishing Simulations**: Run periodic phishing simulations to test employee vigilance and preparedness. Use tools like **Cyber Range** for training.
  + **User Awareness Programs**: Increase the frequency of phishing awareness training, ensuring all employees are aware of the latest phishing tactics.

**Recommendations for Improvement**

* **Enhanced Training**: Conduct more frequent and realistic phishing simulations to improve employee recognition of phishing attempts.
* **Email Security**: Implement more advanced email filtering technologies, including DMARC, to better validate emails and prevent spoofing.
* **Multi-Factor Authentication (MFA)**: Require MFA for all accounts, especially those with sensitive data, to mitigate the impact of compromised credentials.
* **Regular Incident Drills**: Engage in more regular incident response exercises, such as those offered by **SANS NetWars**, to ensure preparedness for real-world attacks.