# **Incident Response Plan Template – Phishing Email Attack with Image-Based Payload**A picture containing dark, holding, sitting, light Description automatically generated

**1. Introduction**

This plan addresses a phishing email attack where an image file contains a hidden payload. When opened, the payload establishes a reverse shell, granting the attacker remote access, and may encrypt files with ransomware. The objective is to detect, contain, eradicate, recover from, and prevent such incidents.

**2. Incident Identification & Initial Response**

**Detection Methods**

* Email security solutions flagging suspicious image attachments.
* Antivirus software detecting malicious code within image files.
* User reports of suspicious emails or unusual system behavior.

**Immediate Actions**

* Isolate affected machines from the network.
* Notify IT Security and SOC teams.
* Alert employees about the phishing campaign.

3. Containment & Eradication

**Key Steps**

* Analyze the image payload with forensic tools to assess its behavior and impact.
* Block the email sender’s domain and any associated malicious URLs.
* Scan affected systems for malware logs and remove malicious files or processes.
* Revoke compromised credentials to prevent further access.

**Tools Used**

* **Threat Intelligence Platforms:** VirusTotal for payload analysis.
* **Windows System Tools:** Sysmon and Event Viewer for system activity monitoring.
* **Malware Analysis Tools:** For dissecting the payload.
* **Network Security Solutions:** SIEM (e.g., Splunk) and firewalls to block malicious traffic.

**4. Recovery & Remediation**

- Restore affected devices from clean backups, verifying system integrity against known baselines.

- Remove persistence mechanisms (e.g., scripts, scheduled tasks, or registry changes) left by the attacker.

- Conduct a root cause analysis to identify how the payload was concealed in the image and improve detection.

- Patch vulnerabilities, update software, and strengthen PowerShell settings (e.g., script signing, restricted access).

- Enhance monitoring with increased PowerShell logging and file integrity checks.

- Communicate incident details and recovery updates to stakeholders (users, IT teams, executives).

- Perform post-recovery testing to confirm no attack remnants remain.

- Implement defenses like advanced email filtering, attachment scanning, and application whitelisting.

# Workplace Awareness: Importance and How to Achieve It

## Introduction

Awareness in the workplace, especially in areas like security and safety, is the first line of defense against internal and external threats. Organizations today face risks not just from outside attacks but from uninformed decisions and careless behavior within.

## Importance of Awareness

1. Prevents Losses: Lack of awareness has led to major incidents. For instance, computer viruses cause losses in the millions globally.

2. Reduces Human Errors: Many security breaches stem from social engineering and phishing that exploit unaware employees.

3. Strengthens Organizational Security: Aware workers can detect threats early and act swiftly to prevent damage.

4. Supports Compliance: Many standards (like ISO, HIPAA, GDPR) require continuous awareness training.

## Types of Security Threats That Require Awareness

- Phishing Attacks (Email, Spear Phishing, Smishing)

- Social Media Scams

- Password Breaches

- Malware Infections

- Ransomware Attacks

## Best Practices to Build Awareness Among Workers

1. Regular Training Programs:  
 - Conduct interactive sessions  
 - Use real-life scenarios and simulations

2. Visual Campaigns:  
 - Posters, banners, and desktop wallpapers about security tips

3. Email Newsletters:  
 - Monthly awareness tips and recent incidents

4. Phishing Simulations:  
 - Test employees with simulated phishing emails to assess alertness

5. Use of Policies and Reminders:  
 - Share clear guidelines on password management, email use, and USB restrictions

6. Multi-Factor Authentication:  
 - Encourage secure logins for all systems

7. Reporting Culture:  
 - Create a safe channel to report suspicious emails or activity

**Engaging Awareness Games for Workers**

**1. Google's Phishing Quiz**

This interactive quiz by Google tests your ability to identify phishing emails. You're shown examples of real and fake emails and asked to decide which is which. It's an excellent way to raise awareness about email scams in a fun, educational way.

Play here: https://phishingquiz.withgoogle.com

**2. The Weakest Link: A User Security Game**

A game that places you in the shoes of an employee making decisions that affect company security. It provides real-world scenarios and instant feedback on the choices you make, helping to reinforce good security behavior.

Play here: https://www.isdecisions.com/user-security-awareness-game/

**3. CDSE Security Awareness Games**

A variety of games provided by the U.S. Department of Defense to promote security awareness in areas such as password management, physical security, and data protection. These games are suitable for both individuals and teams.

Play here: https://www.cdse.edu/Training/Security-Awareness-Games/

**4. Phishing IQ Test by PhishingBox**

This quiz challenges your knowledge of phishing tactics using real-life examples. It’s a great way to self-evaluate and improve your ability to recognize cyber threats.

Play here: https://www.phishingbox.com/phishing-test

**5. Terranova Security Cyber Games**

Terranova offers gamified security awareness experiences that simulate workplace scenarios. Participants make security-related decisions and learn from the consequences, encouraging better behavior.

Play here: https://www.terranovasecurity.com/products/security-awareness-platform/cyber-games/play

## Conclusion

Awareness is not a one-time event—it is a continuous culture of learning, adapting, and protecting. Empowering employees through consistent, engaging, and practical education leads to a more secure and resilient workplace.