

# Eradication of Email Security Incidents Checklist

**Note:** Prior to starting the eradication of email security incidents checklist, Section 1 and Section 2 must be filled with required information.

## Section 1: Details of the Organization

|  |  |
|--|--|
| Organization Name:                     |  |
| Contact Number:                        |  |
| Website:                               |  |
| Address:                               |  |
| <i>Additional Contact Information:</i> |  |
|  |  |

## Section 2: Details of the Incident Responder

|   |        |  |                               |  |
|---|--------|--|-------------------------------|--|
| Date Received:                              | Report |  | Date Report Processing Began: |  |
| Name:                                       |        |  | Report Number:                |  |
| Title:                                      |        |  | Department:                   |  |
| Email Address:                              |        |  |                               |  |
| Phone Number and, if Applicable, Extension: |        |  |                               |  |
| <i>Additional Details (If any):</i>         |        |  |                               |  |

| Section 3: Eradication of Email Security Incidents Checklist   |                          |
|--|--------------------------|
| Actions  | Completed                |
| Whether the details of an email security incident, such as URL, hostname, subject link, sender, and IP address, from email header analysis are collected and blocked across servers, security tools, and network devices | <input type="checkbox"/> |
| Whether employees are alerted about the incident and trained to diagnose those alerts  | <input type="checkbox"/> |
| Whether the antiphishing and antispam tools are updated with the newly found signatures and details of the attackers to prevent similar attacks in the future  | <input type="checkbox"/> |
| Whether common patterns and signatures from the emails are identified and blocked on the SMTP server   | <input type="checkbox"/> |
| Whether the SMTP logs are reviewed to determine if the attackers have sent the same or similar emails to other employees and removed them from the inboxes   | <input type="checkbox"/> |
| Whether the impact of the attacks on other users are checked and incident handling processes are performed on their systems as well  | <input type="checkbox"/> |
| Whether DNS black holing is used to block IP addresses   | <input type="checkbox"/> |
| Whether the security of email servers and clients are hardened   | <input type="checkbox"/> |
| Whether the email incident reports are shared with peers through forums and submitted them to online databases and authorities   | <input type="checkbox"/> |
| Whether employees are trained to check email headers for those emails asking for immediate actions, such as financial transactions   | <input type="checkbox"/> |
| Whether multiple verification policies are implemented for financial transactions  | <input type="checkbox"/> |
| Whether malicious websites are blacklisted and automatic downloads across all the systems and devices are disabled   | <input type="checkbox"/> |
| Whether all affected systems are scanned using next-generation antivirus to ensure the removal of all malware-related data   | <input type="checkbox"/> |
| Whether the impacted accounts are blocked and removed and new accounts to the employees are re-issued  | <input type="checkbox"/> |
| Whether all employees are requested to change their passwords and multi-factor authentication is implemented for their accounts  | <input type="checkbox"/> |
| Whether browser extensions and tools are installed that help in detecting and preventing phishing and spam emails  | <input type="checkbox"/> |

|   |                          |
|---|--------------------------|
| Whether the email using signatures, sender's addresses, or other details of any malicious email is blacklisted  | <input type="checkbox"/> |
| Whether encryption or VPNs are used to communicate using emails   | <input type="checkbox"/> |
| Whether antispam, antiphishing, and filtering tools such as SPAMfighter, SpamTitan, and MailWasher are deployed | <input type="checkbox"/> |
| Whether regional law enforcement agencies are informed about fraudulent emails                                  | <input type="checkbox"/> |
| Whether the vulnerabilities exploited by the malware to corrupt the systems and other devices are patched       | <input type="checkbox"/> |
| Whether the root cause analysis of the incident is performed  | <input type="checkbox"/> |
| Whether the old software versions are updated   | <input type="checkbox"/> |
| Whether the gaps in security controls are identified and resolved   | <input type="checkbox"/> |
| Whether the activity of affected user accounts is monitored after resetting the passwords                       | <input type="checkbox"/> |
| Check whether the DNS logs are reviewed to find which user accounts accessed the identified malicious domains   | <input type="checkbox"/> |
| Check whether the affected systems are restored with a trusted backup   | <input type="checkbox"/> |