Rick Abraham

My Company  Dallas, TX

Risk Assessment – Phishing and Social Engineering Risks

Contents

[Introduction 2](#_Toc182579278)

[Purpose 2](#_Toc182579279)

[Scope 2](#_Toc182579280)

[Risk Identification 2](#_Toc182579281)

[Risk Analysis 3](#_Toc182579282)

[Mitigation Recommendations 3](#_Toc182579283)

[Employee Email Accounts 3](#_Toc182579284)

[Messaging Platforms 3](#_Toc182579285)

[Phone/Voicemail Systems 4](#_Toc182579286)

[Executive Email Accounts 4](#_Toc182579287)

[Vendor/Third-Party Access 4](#_Toc182579288)

[Monitoring and Review 4](#_Toc182579289)

[Frequency 4](#_Toc182579290)

[Daily 4](#_Toc182579291)

[Monthly 5](#_Toc182579292)

[Quarterly 5](#_Toc182579293)

[Bi-Annually 5](#_Toc182579294)

[Annually 5](#_Toc182579295)

[Incident Response 5](#_Toc182579296)

[Documentation and Compliance 6](#_Toc182579297)

Risk Assessment – Phishing and Social Engineering Risks

# Introduction

Purpose: This risk assessment identifies threats related to phishing and social engineering attacks that target employees and systems. It evaluates vulnerabilities, their potential impact, and provides strategies to mitigate risks and enhance organizational resilience.

Scope: Covers all communication platforms including email, messaging apps, collaboration tools, phone calls, and any human-targeted attack vectors.

# Risk Identification

| **Asset** | **Threat** | **Vulnerability** | **Impact** | **Risk Rating** |
| --- | --- | --- | --- | --- |
| Employee Email Accounts | Phishing emails designed to steal credentials | Lack of email filtering, employee unawareness | Unauthorized access, data breaches | High |
| Messaging Platforms | Social engineering attacks via collaboration tools | Lack of message monitoring and awareness training | Malicious links, malware distribution | High |
| Phone/Voicemail Systems | Vishing (voice phishing) attacks targeting employees | Lack of multi-factor authentication and verification policies | Unauthorized financial transactions, credential theft | Medium |
| Executive Email Accounts | Spear-phishing targeting executives (CEO fraud) | Lack of DMARC protocols and impersonation detection | Large financial losses, reputational damage | High |
| Vendor/Third-Party Access | Phishing attacks impersonating vendors | Inadequate vendor verification processes | Unauthorized access, supply chain disruptions | Medium |

# Risk Analysis

| **Asset** | **Likelihood** | **Impact Severity** | **Overall Risk Level** |
| --- | --- | --- | --- |
| Employee Email Accounts | High | High | Critical |
| Messaging Platforms | Medium | Medium | Moderate |
| Phone/Voicemail Systems | Medium | Medium | Moderate |
| Executive Email Accounts | High | High | Critical |
| Vendor/Third-Party Access | Medium | High | High |

# Mitigation Recommendations

## Employee Email Accounts

* Deploy **email filtering tools** with machine learning capabilities to block phishing emails before they reach inboxes.
* Implement **multi-factor authentication (MFA)** for all email logins to prevent unauthorized access even if credentials are compromised.
* Conduct **regular phishing awareness training**, including simulated phishing campaigns, to teach employees how to identify suspicious emails.

## Messaging Platforms

* Enable **link scanning tools** to detect and block malicious links shared via collaboration platforms (e.g., Teams, Slack).
* Monitor file-sharing activities for unauthorized or suspicious file uploads.
* Educate employees on recognizing social engineering attempts and reporting suspicious messages.

## Phone/Voicemail Systems

* Require **verbal verification protocols** for sensitive transactions initiated over the phone.
* Implement **call-back policies** where employees verify requests by contacting the requester using pre-approved contact information.
* Use **caller ID spoofing detection tools** to identify fraudulent calls.

## Executive Email Accounts

* Apply **DMARC, SPF, and DKIM protocols** to prevent email spoofing and impersonation of executive accounts.
* Monitor executive accounts for unusual login activity or messages requesting sensitive information.
* Educate executives on the unique risks of spear-phishing and provide personalized security support.

## Vendor/Third-Party Access

* Verify all requests from vendors through **independent communication channels** before responding.
* Limit vendor access to critical systems through **least privilege principles** and regularly audit permissions.
* Incorporate **vendor-specific phishing awareness** into onboarding and periodic training.

# Monitoring and Review

Frequency

### Daily

* Monitor email filtering systems for blocked phishing attempts and review logs for failed login attempts.
* Track flagged messages in collaboration tools (e.g., Teams, Slack) for suspicious content or links.

### Monthly

* Review phishing simulation reports to measure employee susceptibility and identify at-risk departments.
* Audit logs from email servers and authentication systems to detect abnormal login patterns.

### Quarterly

* Audit permissions and shared access across email accounts and collaboration tools, removing unused or unnecessary access.
* Review metrics from advanced threat protection tools to detect new trends in phishing attempts.

### Bi-Annually

* Conduct a **comprehensive phishing simulation drill** across all departments, targeting various attack vectors (e.g., email, phone, and collaboration platforms).
* Evaluate the effectiveness of current anti-phishing tools, such as email filtering and link scanning systems, and compare against the latest industry benchmarks.
* Perform **tabletop exercises** with the Phishing Response Team (PRT) to simulate phishing incidents and evaluate response protocols. Update playbooks based on lessons learned.
* Assess vendor security protocols and conduct a **third-party phishing risk audit**, focusing on communication channels and access policies.

### Annually

* Reassess the overall phishing risk landscape, incorporating the latest trends, such as deepfake audio for vishing or AI-driven phishing emails.
* Update organization-wide phishing awareness training materials to reflect emerging attack techniques.
* Evaluate organizational compliance with regulatory requirements, including GDPR and NIST guidelines.

Incident Response

* Establish a **Phishing Response Team (PRT)** and conduct bi-annual tabletop exercises to improve readiness.
* Develop a bi-annual **Incident Response Summary Report**, which includes:
  + The number of phishing incidents reported.
  + Response times and remediation outcomes.
  + Identified gaps in current response protocols.
* Test phishing-related breach escalation processes every six months, ensuring alignment with regulatory notification timelines.

Documentation and Compliance

* Maintain detailed logs of phishing incidents, including type, source, affected systems, and remediation actions taken.
* Document all updates to email filtering configurations, link scanning tools, and endpoint protection measures.
* Record phishing simulation results, including employee susceptibility rates and training outcomes, to track progress and improve defenses.
* Ensure compliance with applicable cybersecurity regulations and standards, including:
  + **NIST SP 800-53**: AC-2 (Access Control), SI-4 (System Monitoring), AT-2 (Training), and IR-4 (Incident Response).
  + GDPR, CCPA, and other data protection frameworks.
* Maintain audit trails for email filtering systems, collaboration tools, and anti-phishing software configurations.
* Regularly review and update phishing awareness training materials to reflect emerging social engineering techniques.