EMAIL SECURITY CHECKLIST

Prepared by HANIM EKEN

https://ie.linkedin.com/in/hanimeken

It is a checklist for email security to help safeguard against various threats:

Email Authentication:

- Implement email authentication protocols such as SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) to prevent email spoofing.

Anti-Phishing Measures:

- Educate users about phishing threats and provide regular training to recognize phishing emails.
- Deploy anti-phishing tools and technologies to detect and block phishing attempts.

Email Encryption:

- Enable email encryption, especially for sensitive and confidential information.
- Ensure that end-to-end encryption is used for secure communication.

Secure Password Policies:

- Enforce strong password policies for email accounts.
- Encourage the use of multi-factor authentication (MFA) for an additional layer of security.

Email Filtering:

- Utilize email filtering solutions to identify and block spam, malicious attachments, and links.
- Regularly update and maintain the email filtering rules and databases.

User Awareness Training:

- Conduct regular training sessions to educate users about email security best practices.
- Instruct users not to click on suspicious links or download attachments from unknown sources.

Secure Email Gateways:

- Implement secure email gateways to scan and filter inbound and outbound emails for malware, viruses, and other threats.
- Configure email filtering policies to block malicious content.

Email Archiving:

- Set up email archiving to retain and store emails securely for compliance and legal purposes.
- Ensure that archived emails are easily retrievable when needed.

Mobile Device Security:

- Implement security measures for mobile devices accessing corporate email accounts.
- Enable remote wipe capabilities for lost or stolen devices to protect sensitive data.

Regular Software Updates:

- Keep email servers, clients, and security software up-to-date with the latest patches and updates.
- Regularly review and update email security configurations.

Incident Response Plan:

- Develop and maintain an incident response plan specific to email security incidents.
- Ensure employees know the reporting procedures for suspected email security incidents.

Email Access Control:

- Restrict access to email accounts based on job roles and responsibilities.
- Monitor and audit email access to detect and respond to any unauthorized access.

Data Loss Prevention (DLP):

- Implement DLP measures to prevent the unauthorized transmission of sensitive or confidential information via email.
- Regularly review and update DLP policies to align with organizational needs.

Legal and Regulatory Compliance:

- Ensure email security measures comply with relevant laws and regulations, such as GDPR, HIPAA, or industry-specific standards.
- Conduct periodic compliance audits to verify adherence to email security requirements.

HANIM EKEN

https://ie.linkedin.com/in/hanimeken