PROTECTION CHECKLIST FOR PHISHING EMAIL

Prepared by HANIM EKEN

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

Here's a checklist to help protect against phishing emails:

User Education and Training:

- Provide regular training to educate users about the dangers of phishing.
- Teach users how to recognize phishing emails, including common tactics used by attackers.

Email Authentication:

- Implement SPF, DKIM, and DMARC to authenticate emails and prevent email spoofing.
- Configure DMARC policies to specify how to handle unauthenticated emails.

Anti-Phishing Software:

- Deploy advanced anti-phishing solutions to detect and block phishing emails.
- Ensure that the software is regularly updated with the latest phishing threat intelligence.

Email Filtering:

- Utilize email filtering tools to identify and block phishing emails before they reach users' inboxes.
- Configure strong filtering rules to catch suspicious content.

Secure Email Gateways:

- Implement secure email gateways to scan emails for malicious links, attachments, and content.
- Configure gateway settings to block or quarantine suspicious emails.

Multi-Factor Authentication (MFA):

- Encourage or enforce the use of multi-factor authentication for email accounts.
- MFA adds an extra layer of security even if login credentials are compromised.

Check Sender Details:

- Train users to carefully check sender email addresses for inconsistencies or slight variations.
- Avoid clicking on links or downloading attachments from unknown or suspicious senders.

Verify Unexpected Emails:

- Encourage users to verify unexpected emails by contacting the supposed sender through a known and trusted communication channel before taking any action.

Hover Over Links:

- Instruct users to hover over links in emails to preview the destination URL before clicking.
- Verify that the URL matches the expected domain.

Avoid Personal Information Sharing:

- Emphasize the importance of not sharing sensitive personal or financial information via email.
- Remind users that legitimate organizations will not request such information through email.

Incident Reporting:

- Establish clear procedures for reporting suspected phishing emails.
- Encourage users to report any suspicious emails promptly to the IT or security team.

Regular Simulated Phishing Exercises:

- Conduct regular simulated phishing exercises to assess user awareness and responsiveness.
- Use the results to further tailor training and awareness programs.

Email Encryption for Sensitive Information:

- Implement email encryption for sensitive information to protect it from unauthorized access in case of a phishing attack.

Regular Security Updates:

- Keep email clients, browsers, and security software up-to-date to benefit from the latest security patches.
- Regularly update and patch the operating system and other software.

Monitoring and Incident Response:

- Implement continuous monitoring for phishing attempts and unusual email activity.
- Have an incident response plan in place to quickly address and mitigate phishing incidents.

HANIM EKEN

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