

LetsDefend
Phishing Playbook



letsdefend.io

START

Parse Email

- 1-When was it sent?
- 2-What is the SMTP address of the email?
- 3-What is the sender's address?
- 4-What is the recipient's address?
- 5-Is the content of the email suspicious?
- 6-Are there any attachments?

Are there attachments or URLs in the email?

YES

Analyze URL/Attachment

You can use the free products/ services below.

- AnyRun
- Virus Total
- Hybrid Analysis

Is the file/url malicious?

YES

Has the email been delivered to the user?

YES

Action

Delete e-mail from recipient.

Was the malicious file or URL opened?

YES

Header Analysis

- Download and analyze the EML file from email security.
 - Filtering based on DKIM + SPF or header analysis. Header analysis can help detect if the email sender is spoofed.
- Was the email spoofed?

YES/NO

Containment

The systems that were exposed to the cyber attack should be isolated and the impact of the cyber attack should be reduced.

Lesson Learned

- How did the cyber attack happen?
- How well did staff and management deal with the incident?
- What could staff and management do differently next time a similar incident occurs?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?

Artifacts

Note any artifacts found while investigating.

Analyst Note

Please enter your comments on the analysis.

START