OVERVIEW

CISA’s Phishing Campaign Assessment (PCA) measures a workforce’s tendency to click on email phishing lures. Malicious cyber actors commonly use phishing to collect sensitive information or to obtain initial access to a network. Based on CISA testing, phishing is the number one means of malicious cyber actors obtaining initial access into a private network. Stakeholders can use PCA results to inform the anti-phishing training and awareness that they provide to their workforce.

PCA is designed to:

- **Test** and assess the behavioral responses of a specified target user base when presented with expertly crafted phishing emails emulating real world threats.
- **Inform** leadership of potential training and awareness improvements based on the metrics gathered through the course of the assessment.

OBJECTIVES

- Reduce risk to malicious phishing email attempts by testing and informing users.
- Understand how users are enticed to click on links and report suspicious activity.
- Emulate malicious phishing activity to provide a quality learning experience.

PHASES

<table>
<thead>
<tr>
<th>Phase</th>
<th>Pre-Planning</th>
<th>Planning</th>
<th>Execution</th>
<th>Post-Execution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stakeholder:</td>
<td>• Requests service.</td>
<td>• CISA confirms schedule.</td>
<td>• CISA sends increasingly deceptive phishing emails from -approved templates.</td>
<td>• Provides weekly click-rate summaries.</td>
</tr>
<tr>
<td></td>
<td>• Receives PCA briefing documents.</td>
<td>• Stakeholder approves email templates.</td>
<td></td>
<td>• Provides final review and report.</td>
</tr>
<tr>
<td></td>
<td>• Signs and returns documents.</td>
<td>• CISA tests email delivery/receipt.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

HOW TO GET STARTED

Contact [vulnerability@cisa.dhs.gov](mailto:vulnerability@cisa.dhs.gov) to get started. Please keep in mind:

- CISA’s assessments are available to both public and private organizations at no cost.
- Service availability is limited; service delivery timelines are available upon request. CISA prioritizes service delivery queues on a continuous basis to ensure no stakeholder/sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.