CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

PHISHING CAMPAIGN ASSESSMENT

The CISA team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA's Phishing Campaign Assessment (PCA) measures an organization's propensity to click on email phishing lures, commonly used to collect sensitive information or as initial access to a network. Based on CISA testing, email phishing is the number one means of initial access into a private network. PCA results can be used to provide guidance for anti-phishing training and awareness.

CAPABILITIES

Test: Assess the behavioral responses of a specified target user base when presented with expertly crafted phishing emails emulating real world threats.

Inform: Provide leadership information on potential training and awareness improvements based on the metrics gathered through the course of the assessment.

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
- Properly emulate malicious phishing activity to provide a quality learning experience

ASSESSMENT TIMELINE

Pre-Planning

- Request assessment
- Receive PCA briefing documents
- Sign and return forms

Planning

- Confirm schedule
- Approve email templates
- Test email delivery/receipt

Execution (Six weeks)

- Receive increasingly deceptive phishing emails from pre-approved templates

Post-Execution

- Receive weekly click-rate summaries
- Final report review and receipt
- Optional retest available

ABOUT

Our Team

The CISA team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities.

Additional Information

CISA's security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.

GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at **vulnerability_info@cisa.dhs.gov** to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.

MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation’s cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*