Phishing Exercises

Do's and Don'ts

Do's:

- Obtain approval for any phishing exercise, and your phishing email templates, from your Information Security Officer (ISO) and Agency Information Security Officer (AISO)!*
- Notify the California Cybersecurity Integration Center (Cal-CSIC) at CalCSIC.SecurityAlerts@caloes.ca.gov and the California Department of Technology, Office of Information Security (CDT-OIS) at security@state.ca.gov at least 72 hours before the exercise. Notification must include the proposed email(s) to be used.
- Have a complete exercise plan that includes:
    - Use of fictional entity name(s), brand/logo(s), image(s), etc.
    - Pre and post exercise communication messages and protocols.
    - Information that reinforces the information/instructions a user will have received from awareness training, such as looking for poor grammar, typos, etc.
    - Pre- and post-exercise steps to control and properly manage the test. For example, controlling test emails from being forwarded outside the test entity and ensuring their removal from employee email/shared email boxes once exercise is completed.
    - Advance notice to the business areas most likely impacted by the testing activity, such as IT help desk, entity ISO Office, etc.
    - When appropriate, segment exercises and align with learner groups by functional role. A role-based approach will also minimize impact on day-to-day business activities and processes.
    - Assignment of observers/notetakers for the testing activity or application logs to ensure the capture of various types of responses and lessons learned.
- Try to use phishing emails that have previously been seen "in the wild" when possible to better mimic threats users will face.

Don'ts:

- NEVER initiate a phishing exercise without first providing the required 72 hour advance notification to Cal-CSIC and CDT-OIS.
- Don't use inappropriate or sensitive material for phishing emails. The use of union names, legal or contractual issues, political themes, or commercial trademarks without approval, should be avoided.

**Note: All California Military Department Independent Security Assessment phishing emails are approved through the CDT Office of Information Security.*