Policy and Procedure

|  |
| --- |
| Internal Services Division |

|  |  |
| --- | --- |
| To: | David O’Toole, Jeff Vail |
| From: | Catherine Wild – Principal IT Analyst |
|  | Marty Feldmann – IT Customer Services Manager |
| Date: | 3/20/2019 |
| Re: | **Email Phishing Security Testing** |
| Comments: | Listed below are the procedure points for email phishing security testing at the Districts.   1. The Sanitation Districts will undergo phishing testing twice a year, with Regional San (including central service departments) tested in the first and third quarter of the calendar year, and SASD tested in the second and fourth Approximately one-half of Regional San and SASD will be tested each quarter. The frequency of testing may be increased based on test results. 2. The phishing template will be selected by the ISD Director, with input from the Information Security Officer and Customer Services Manager. The District Engineer will provide final approval. All Securing the Human templates have been reviewed by HR-Labor Relations and the Department of Technology. 3. An initial pilot phishing test will be sent to the Customer Services team for testing and verification, ahead of delivery to the Districts’ staff. (Other IT staff will be included in regular testing groups.)  Once the pilot test is complete and satisfactory, the Customer Services Manager will partner with the Information Security Officer to specify a list of staff to be included in each of the groups identified for the bi-annual phishing exercise. They will also select the date and time of execution, with a starting day of Tuesday during the week selected. 4. A final confirmation email will be sent from the Security Team to the IT Customer Services staff one business day prior to deployment. 5. The security team will phish each group on the list, as selected, per the predetermined schedule. 6. The security team will set the end date (date to stop recording the phishing campaign) five working days from the start date. 7. The security team will provide reports to management within five working days after the completion of phishing both districts.   Tech Team guidelines for response to customer queries are as follows:   * Thank you for reporting the suspicious email. This particular one has been reported to the information security team so you can shift delete it if you have not done so already. * Please continue to call us anytime you have a question about a suspicious email.  (Promotes customer call-back in the future when questions arise) * Tech will verify the email is from the district’s phishing test. * This is a test as part of our Security training. * Please do not inform your colleagues about this email, as it would skew our test results. * If customers inquire about further tests, Tech will remain noncommittal in response, to encourage customer vigilance in the future. |