WEST VALLEY WATER DISTRICT
855 W. Base Line Road Rialto, CA 92376
PH: (909) 875-1804 FAX: (909) 875-1849

SPECIAL SAFETY & TECHNOLOGY COMMITTEE MEETING AGENDA

MONDAY, AUGUST 30TH- 6:00 PM

NOTICE IS HEREBY GIVEN that West Valley Water District has called a meeting of the Safety & Technology Committee to meet in the Administrative Conference Room, 855 W. Base Line Road, Rialto, CA 92376.

Teleconference Notice: In an effort to prevent the spread of COVID-19 (Coronavirus), and in accordance with the Governor's Executive Order N-29-20 and the order of the County of San Bernardino dated March 17, 2020, there will be no public location for attending this Committee Meeting in person. Members of the public may listen and provide public comment via telephone by calling the following number and access code: Dial: (888) 475-4499, Access Code: 840-293-7790 or you may join the meeting using Zoom by clicking this link: https://us02web.zoom.us/j/8402937790. Public comment may also be submitted via email to administration@wvwd.org. If you require additional assistance, please contact the Executive Assistant at administration@wvwd.org.

BOARD OF DIRECTORS

Director Dr. Michael Taylor (Chair)

Director Kyle Crowther

1. CONVENE MEETING

2. PUBLIC PARTICIPATION

The public may address the Board on matters within its jurisdiction. Speakers are requested to keep their comments to no more than three (3) minutes. However, the Board of Directors is prohibited by State Law to take action on items not included on the printed agenda.

3. DISCUSSION ITEMS

A. General Updates to Safety Committee

B. Report on Internal Phishing Campaign

4. ADJOURN

DECLARATION OF POSTING:

I declare under penalty of perjury, that I am employed by the West Valley Water District and posted the foregoing Finance Committee Agenda at the District Offices on August 25th, 2021.

Maisha Mesa, Executive Assistant

BOARD OF DIRECTORS
SAFETY AND TECHNOLOGY COMMITTEE
STAFF REPORT

DATE: August 30, 2021
TO: Safety and Technology Committee
FROM: Shamindra Manbahal , General Manager
SUBJECT: REPORT ON INTERNAL PHISHING CAMPAIGN

BACKGROUND:

Phishing is the fraudulent practice of sending emails (or text messages) pretending to be from reputable companies to trick individuals into revealing personal information such as passwords and credit card numbers.

DISCUSSION:

Recently there has been a noticeable increase in the amount of phishing emails received by West Valley Water District ("District") staff. Most have been directed towards Human Resources and Payroll staff, who have done an exceptional job of identifying them and reporting them. Because all staff are potential targets, the Business Systems/I.T. department initiated an internal phishing campaign, (realistic phishing simulations were developed and sent to staff), to gauge the awareness of staff District-wide. Two campaigns were carried out.

The first campaign was conducted on 08/04/21. The simulated phishing email stated that it was from Office 365 and that there were errors delivering emails to the recipient's inbox. A link was included that opened a website where the recipient was asked to log in. The email contained several red flags that should have helped the recipients to identify that it was fraudulent. For instance, the email claimed to be from Office 365 but was being sent from dUScj@effecturellc.com, which clearly is not from Microsoft.

During the first campaign, one Business Systems/I.T. staff person inadvertently sent an email to all staff warning them not to click on any links in the email. Of the 73 staff who received the emails, 9 clicked on the link and 1 entered their username and password. Those figures were likely lower than what would have occurred naturally because the warning email.

A second campaign was conducted on 08/12/21. The simulated phishing email stated that it was from the "Payroll Admin Department". A link was included that opened a website where the recipient was asked to log in so that they could verify their email account for a new payroll directory and to adjust their monthly benefit payment. Like the previous email, this also included several red flags. For instance, it was sent from Christopher.Lawther@GBMC.ac.uk, and is clearly not from anyone in the District's Payroll Department. The email also referenced adjusting staff's "benefit payment". Staff does not receive any "benefit payments".

Of the 70 staff who received the emails, 8 clicked on the link, (1 person clicked on it twice), and 3 entered their username and password. On a positive note, 19 staff recognized that it was fraudulent and reported it to the Business Systems/I.T. staff. The remaining staff simply ignored the email.

Training on how to identify phishing emails was provided to most of the office staff on 08/17/21. The same training will be repeated for all staff at the next All Hands meeting scheduled for Tuesday, 09/07/21.

FISCAL IMPACT:

The District recently transitioned from Silversky email hosting services to Office 365. Office 365 includes the additional functionality necessary to carry out phishing campaigns There was no cost to the District.

STAFF RECOMMENDATION:

Receive and file.

Respectfully Submitted,

Shamindra Manbahal

Shamindra Manbahal, General Manager

SM:js