OFFICE OF THE INSPECTOR GENERAL

AWARENESS BULLETIN

Date: March 3, 2021

Topic: Compromised LAUSD Email Accounts and Email Scams

The Office of the Inspector General (OIG) has received a recent spike in hotline complaints regarding e-mail scams that originated from LAUSD e-mail accounts. At first glance, these e-mails may appear harmless because the communication is coming from a legitimate LAUSD e-mail account. However, an LAUSD e-mail account can be compromised if an employee clicks on a malicious link, opens an attachment, or completes a form in a phishing email that tricks the employee into providing their username and password, or an employee uses the same password on an unsecure website that was leaked. When an employee's username and password are obtained, hackers may gain unauthorized access, allowing them to send fraudulent emails from that employee's email account.

Social engineering attacks, such as phishing and spoofing, begin with the hacker pretending to be someone or something you know and trust. You can help protect yourself, your family, and our District by recognizing social engineering attacks and mitigating them before they are successful. A good place to start is by watching the following videos from LAUSD IT Security regarding social engineering attacks and passwords.

Social Engineering and Phishing
https://lausd.wistia.com/medias/40isd8wvlf

Passwords
https://lausd.wistia.com/medias/tunkm8lcbm

If your LAUSD e-mail account receives an e-mail that you believe is a social engineering attack, or you believe that your LAUSD e-mail account has been compromised, please report your concern to LAUSD IT Security. You may call the ITD Helpdesk at (213) 241-5200 or send an email to information.security@lausd.net.