Phishing scam asking recipients to validate information appears to target State of Texas licensees

DATE: September 11, 2020

AUSTIN –The Texas Department of Information Resources today announced that an unknown number of people appear to have been targeted with a cyberattack in the form of phishing emails disguised as communications from Texas state agencies. These emails appear to target Texans who have business with that agency and ask the recipient to validate their profile information in state systems. Recipients are falsely told that the agency is requiring all licensees to validate their information no later than Sept. 14, 2020, or their next license renewal could be delayed.

Although the email may appear to originate from legitimate state agencies, none of these emails were actually sent by any Texas government entity. All Texans who receive an email asking licensees to update their profile information are asked to delete the email without clicking on the link or confirming or providing any personal information. Any recipient that has already clicked on the link in the email is advised to reset their account password and those of any other accounts they may have that use the same password.

Relevant agencies have been notified and an investigation is currently ongoing.

Although it appears that the link in question is no longer active, everyone is reminded to protect their personal information while online:

- Never disclose your password to anyone, even a customer service representative purported to represent a state agency or other trusted institution.
- If you are providing personal information to a state agency – or any company – make sure the site is encrypted before providing any personal information. Look for a key or lock on your screen. But do not assume this is safe, be sure you are connected to **Texas.gov.**
- Use unique passwords when setting up an account. Don't re-use passwords and avoid using your date of birth, Social Security number, or simple words as a password. Use a password manager to assist in creating and tracking secure passwords.
- Avoid sending personal information via email unless the security method used is specifically outlined and the data is encrypted.
- Use a secure, modern, and updated web browser.

Texas residents are encouraged to be alert for this and other fraudulent scams.