Texas Department of Information Resources

# Voice to Email Messaging Security Awareness

**March 16, 2020**- In response to the current telework situation, agencies may have enabled Voicemail to Email capability. Using this functionality, a voicemail left on your office phone will be emailed to you as an email with a .wav file attachment. This attachment can then be opened and played back, using your computer or phones audio system.

This functionality comes with an associated risk. Hackers will send an email containing what appears to be a voice to email attachment to you in an attempt to entice users into opening the file. This file, when opened, will then direct you to a phishing site that asks for your credentials. **This redirection and request for credentials is one key indicator that this is a phishing attempt**, as a legitimate voice to email message will not typically prompt you for credentials, as you have already authenticated to the email system itself. Your laptop or phone should simply allow you play the audio message in attached .wav file.

These emails are often very well designed, with an official logo such as Office 365 or other well-known service. It may also appear to be from your own Helpdesk or IT Department. It is important to **carefully check** the visible information in the email before opening an attachment. In most cases, a few seconds of thoughtful consideration will allow you verify the legitimacy of the email and to avoid giving your credentials to a bad actor.

Opening a voice-to-email attachment **SHOULD NOT redirect to a website asking for credentials or other information**. The wav file VoiceMessage.wav file should simply load an audio player and play the file.

If you receive a questionable email and are unsure as to the legitimacy, or if you have received an email and accidentally entered your credentials in an unknown site, contact your information security officer or IT administrator.