Cybersecurity Awareness: smishing

Employees have been made aware about the rise of smishing campaigns that target mobile phone users by sending fake text messages. The text message claims to be from a trusted source, with the sender’s name appearing to be a recognized public entity.

The content of the text message urges recipients to access links and provide certain information required due to the COVID-19 pandemic response.

If an employee suspects they may be have received a smishing text, Information Security Department recommends they take the following steps:

- Check the agency or company’s website for recent updates. Don’t rely on text messages
- Do not click any link within text messages. Instead, click the link from the official website
- Forward suspicious messages to the Communication and Information Technology Commission’s unified number

4/2/2020