
# Don't Get Smished!

- Smishing is another form of social engineering – using text messages to get your private and confidential information!
- Always follow company policy regarding securing your mobile device. *****
- Don't reply to unsolicited text messages.
- Don't "click" on links or open attachments that you are not expecting.
- Don't call phone numbers as directed in text messages. That's a way for smishing to turn into phishing!
- Verify the authentication of a text message or its sender.
- Don't enter sensitive information in a text message – keep your information private.
- When in doubt, don't! Call your Information Security Officer or Network Administrator.

***** For policies about mobile security, visit m.infotex.com/byod.