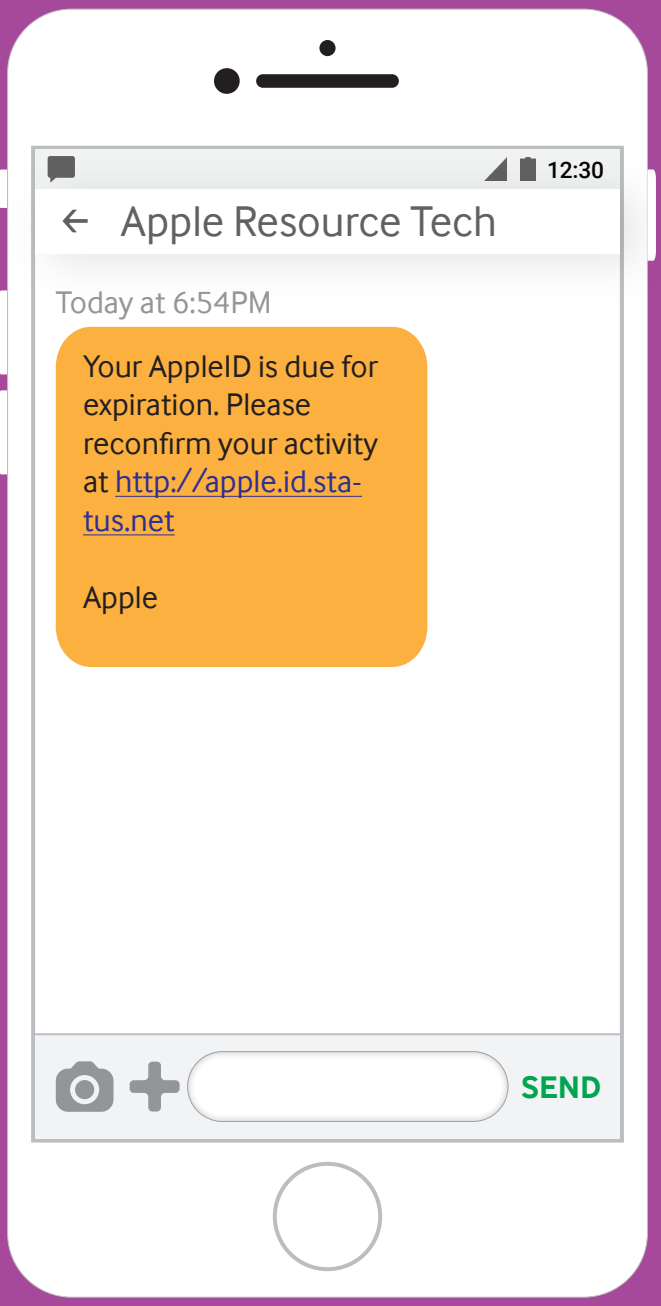
SMISHING

Smishing is phishing – using fraudulent emails to "fish" for victims' personal data – applied to the more intimate world of SMS text messaging.



HOW DOES IT WORK?

The text message will typically ask you to click on a link or call a phone number in order to 'verify', 'update' or 'reactivate' your account.

But the link leads to a bogus website and the phone number leads to a fraudster pretending to be the legitimate company.

A cleverly designed fake website or believable phone call can fool even the tech-saavy into accidentally giving away personal information, making them vulnerable to cyberattacks.

WHAT CAN YOU DO?

- Don't click on links, attachments or images that you receive in unsolicited text messages without first verifying the sender using known contact information.
- Don't be rushed. Take your time and make the appropriate checks before responding.
- Never respond to a text message that requests your PIN or your online banking password or any other security credentials.
- If you think you might have responded to a smishing text and provided your bank details, contact your bank immediately.

Church Educational System
Security Operations Center