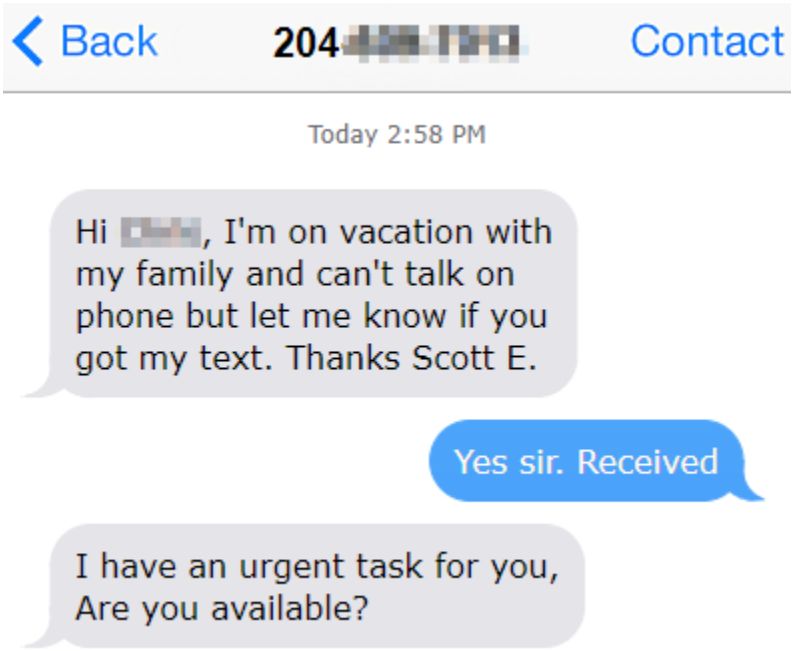
This Month's Tip: SMS Phishing (Smishing) on the Rise!

A form of phishing, known as smishing, is the act of using text messages to trick individuals into disclosing sensitive information, visiting a dangerous website, or downloading a malicious app onto a smartphone. These innocent looking messages may ask to confirm banking details, verify account information, or subscribe to an email newsletter via a link delivered by SMS.
As with phishing emails, the end goal is to trick people into an action that plays into the hands of cybercriminals.

Smishing attempts have risen dramatically, and Supreme Lending employees are in the cross hair. Here is an example of several seen last month:



The good news is that the potential ramifications of these attacks are easy to protect against. In fact, you can keep yourself safe by doing nothing at all. The attack can only do damage if you take the bait.

Here are a few things to keep in mind that will help you protect yourself against smishing:

- Do not click on any link or call any number received from an unknown sender.
- A message from an unknown sender that urges for a quick reply is a clear sign of smishing.
- Never provide personal information such as usernames, banking information, or other account details through text.
- Remember that legitimate companies will not ask for personal information over text.
- Be on the lookout for messages that contain the number "5000" or any number that is not a phone number. These are often associated with email-to-text services that criminals can use to avoid providing an actual phone number.
- Understand that smishing is not limited to just texting – WhatsApp, Facebook, and other messaging services are all potentially vulnerable.

If you have any questions regarding this tip, please contact Information Security via Mark.Nagiel@SupremeLending.com. Thanks for participating in the Information Security effort!