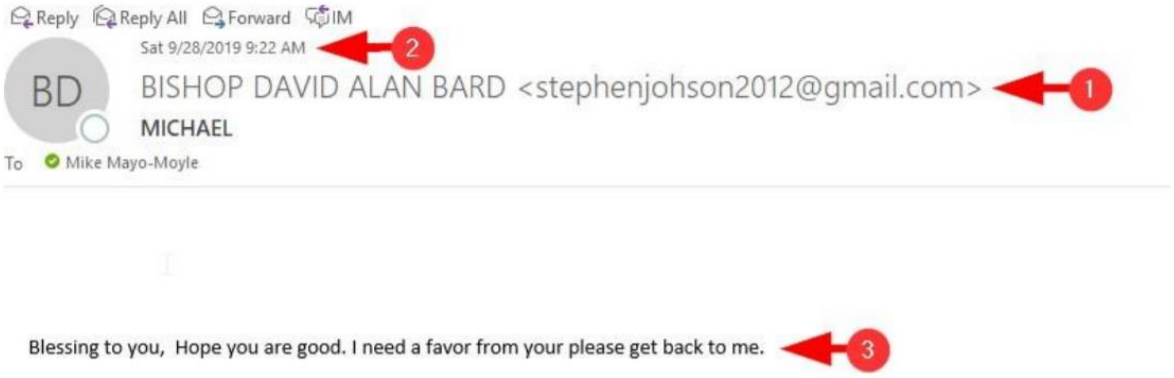
Email Security Information

(Adapted from Conference Communication sent on 10/10/19)

While email provides a wonderful opportunity for quick communication, the underlying technology has the potential to be used maliciously by individuals intending to impersonate and defraud innocent people. We are best served by viewing every email with an air of suspicion, being careful of any small details that might alert us that the sender is not legitimate.

The Michigan conference IT Specialist, Michael Mayo-Moyle, provides the following real-world example of an email he received that was attempting to impersonate Bishop David Bard:



There are a few things to notice:

1. The email isn't originating from Bishop Bard's conference email account. While illegitimate emails may sometimes look very authentic, this is a good thing to watch for. Sometimes, the email address will look right but may be noted as "via" some other address or server.
2. While emails can be sent at any time, an email at 9am on Saturday from Bishop Bard is out of character. It is a good practice to look more carefully at an email that arrives at a strange time or is otherwise outside of the sender's general habits.
3. The body of the email doesn't use Michael Mayo-Moyle's name, despite being addressed to him and his name being in the subject line. Additionally, there are linguistic features that don't match Bishop Bard's usual communication including the grammatical errors (capitalization and punctuation) and the lack of any usual closing or signature.

There are also a few additional "red flags" to look for:

- A sense of urgency ("I need you to reply right away"). Typically, if an issue is urgent the person should try and call you instead.
- Email is offered as the only means of communication ("Don't call, I'm in a meeting right now") in an attempt to keep you from verifying the communication or request.
- The email violates normal financial protocols or practices, such as asking for gift cards to be purchased and sent by email.

If you have any question about the legitimacy of an email, it is best to refrain from additional email communication and communicate directly with the person said to have sent the email. Do not share personal or financial information (gift card serial numbers, credit cards, bank account, etc.) by email.