## **Imposter Scam**

## Please Do Not Fall for the "Imposter Scam"!

I recently was the recipient of an email that reminded me that I should warn those I care about to be aware of and not respond to the various scams that are being attempted.

The email I received appeared to come from our EFCA (denominational) President requesting a confidential personal favor. He let me know he was about to go into a meeting so I should not try calling him but respond by email.

I immediately suspected a scam – but responded to the email asking what I could do for him. The reply I received asked me to purchase \$2,000 worth of Target gift cards, scratch off the backs to reveal the PIN numbers, take pictures of the backs of the cards, and email those pictures to him so he could use the cards to help COVID patients. He let me know that I would "get reimburse" – the bad English in the email being a confirmation of the scam.

Once I received those instructions I knew it was a scam and telephoned our EFCA President to let him know that someone had created a fake email account (even using his picture) and was using that email account to try scamming people.

This attempt to scam me is just one of many variations that crooks are attempting. They often are relatively easy to spot because they contain bad grammar or spelling mistakes – but not always. And, even if the right phone number shows up on your caller ID, that is not proof that someone is not a scammer – because some scammers know how to "spoof" (make it look like they are calling from a different number) phone numbers.

PLEASE know that no one from Mountain View will ever call you, text you, or send you a personal email asking that you do us a favor by sending money directly to us or by purchasing gift cards and sending photos of the card and its PIN, etc. The best thing to do when you receive these requests is to NOT respond to them and contact the person who is supposedly asking for the favor directly using a means of contact that you have used in the past to let them know that you suspect someone is using their name to scam people. It can also be helpful to take note of the return email address of those who contact you via email – as the company associated with those emails (i.e. "gmail") can then be notified of the fake/scammer email account and hopefully shut them down.

-Pastor Bruce