# A few helpful tips for multi-factor authentication

## Instances when you will be prompted for the multi-factor (phone call, text message)

1) Whenever you sign-in to a different network, such as when you are in a different geographical area, you will be asked to type your username (your @ssndcp.org email address) and password.
2) This will be followed by the method you set up for your authentication. That is, either your phone will ring and it will tell you to press the pound key (#), or you will receive a text on your phone with a 6-digit code which you then need to type in the boxes provided on your screen.
3) Once authenticated, you can use your device as usual.

If you ever get a call and are asked to press the pound key when you are **not** trying to sign into a device, **hang up the phone or disregard the text message**, because most likely a hacker was able to go as far as using your password and wants to enter your account.

## If your authentication was set up using the cell phone of a different person (because you don't have a cell phone):

Until we develop a different solution, if you travel from your usual location and you wish to use your iPad or computer to check your @ssndcp.org email, the authentication process will take place. We recommend contacting the person whose phone was used for the authentication *before* you attempt to login, so that when their phone gets a call or text, they will be able to accept it and you will be authenticated. In the case of a text, they will need to tell you the 6-digit code they receive.

## Smartphone and tablet users

We recommend using the Microsoft Outlook app over the default Mail app. As we have found that the Mail app is not reliably notifying folks when they need to authenticate, 'Sign in again,' and has led to day(s) without email for some folks."

Please utilize our guides for steps on installing the Microsoft Outlook app on Apple (iPhone & iPad) devices and for Android (Galaxy, etc)