

INSTRUCTIONS FOR LOGGING-IN TO YOUR MICROSOFT OUTLOOK ACCOUNT (EMAIL)

1. On your desktop computer, open your internet browser (i.e. Microsoft Edge, Google Chrome, Mozilla Firefox) See **Fig. 1**.

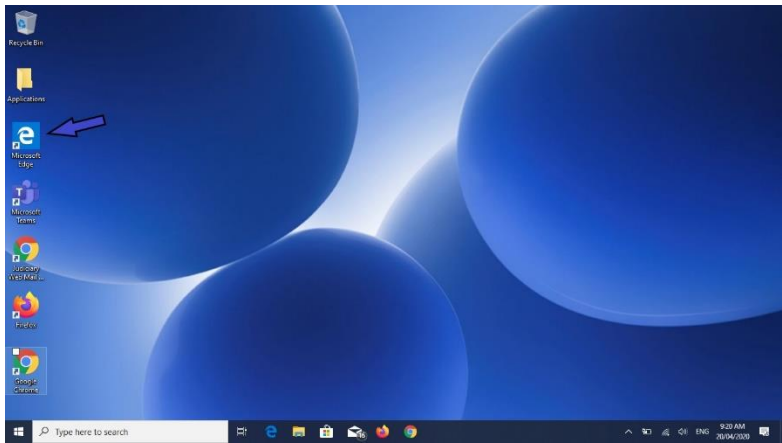


Fig. 1

2. On the address bar, type “outlook.office.com” without the quotation marks and press Enter. See **Fig. 2**.

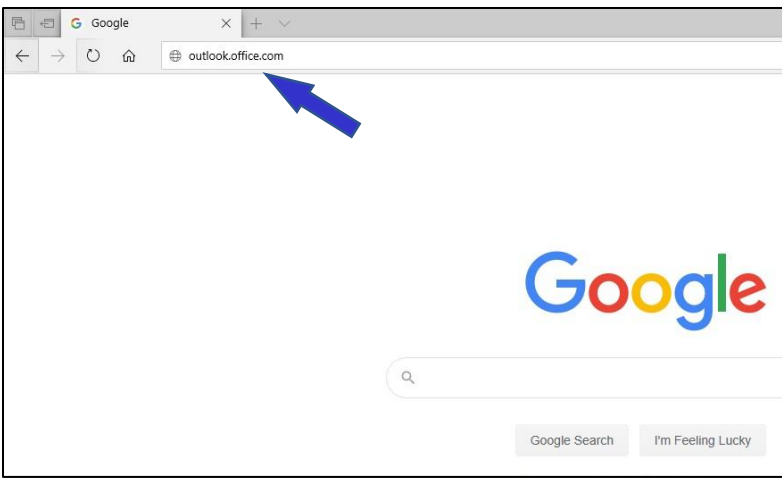


Fig. 2

3. In the Sign in box, type your assigned Microsoft Office 365 email address (for example, rtc1mnlocc@judiciary.gov.ph) and click the Next button. See **Fig. 3**.

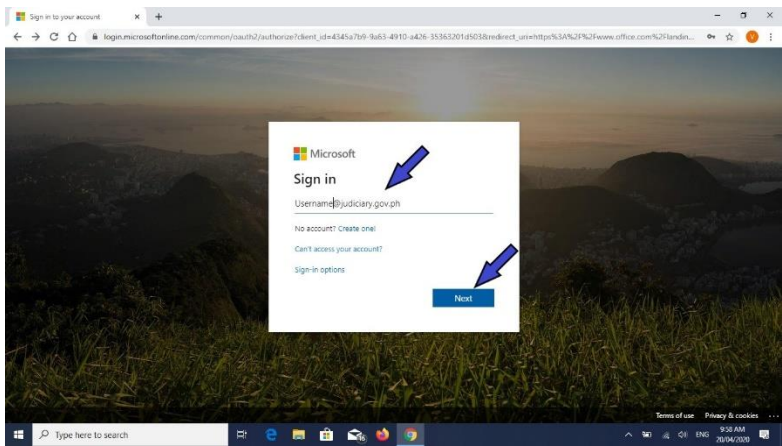


Fig. 3

4. In the Enter password box, type in your assigned password and click the Sign in button. See **Fig. 4**.

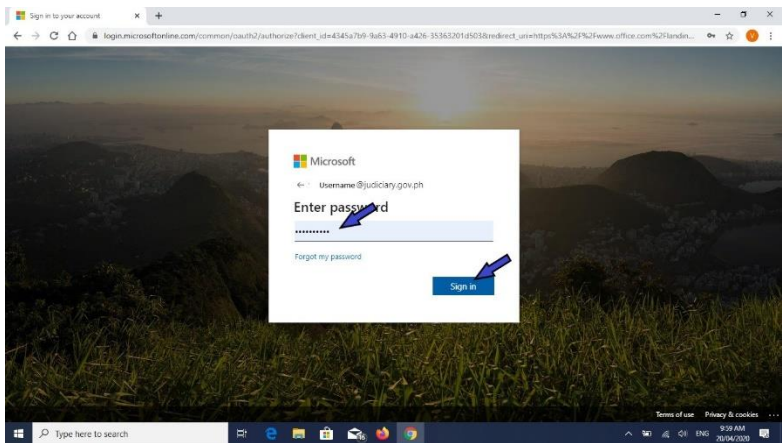


Fig. 4

5. In the Office 365 window page, click on Outlook (email app) on the upper left part of the screen. See **Fig. 5**.

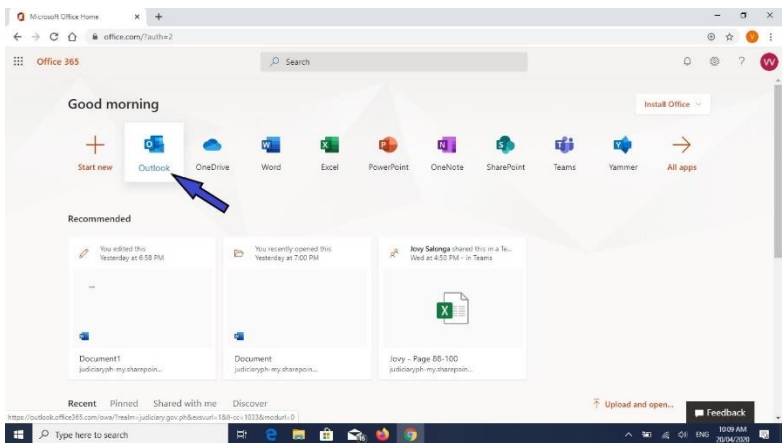


Fig. 5

6. You have now successfully logged-in to your Microsoft Outlook email. See **Fig. 6**.

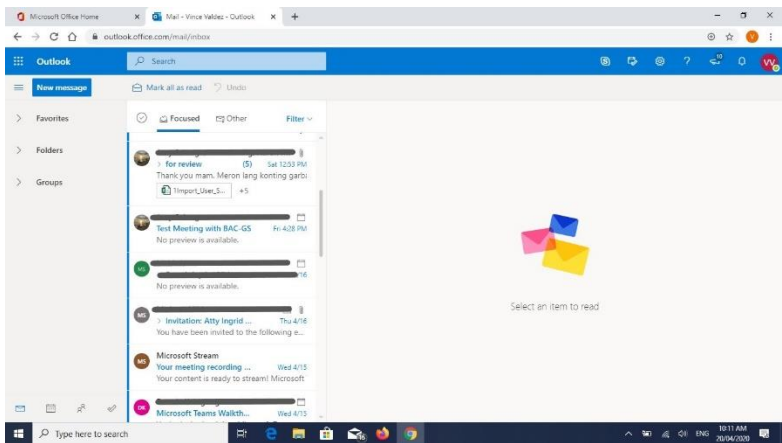


Fig 6.

INSTRUCTIONS ON HOW TO CHANGE YOUR PASSWORD

1. Select the Microsoft Office Home tab on your browser. *See Fig. 7.*

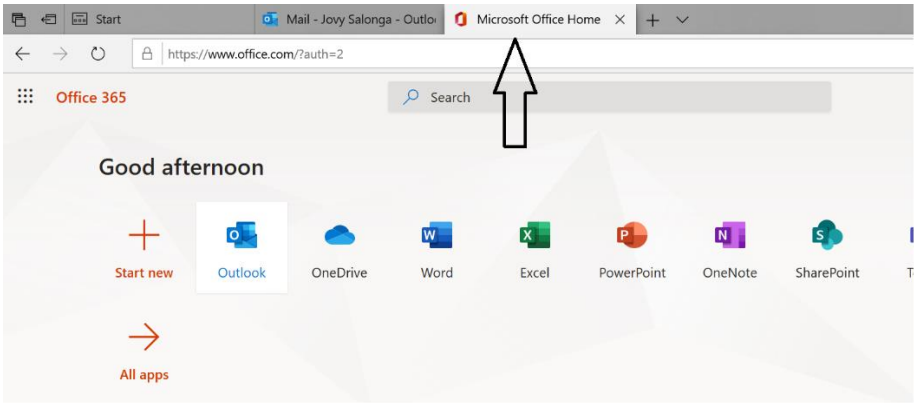


Fig. 7

2. On the upper right portion, click the Settings button. *See Fig. 8.*

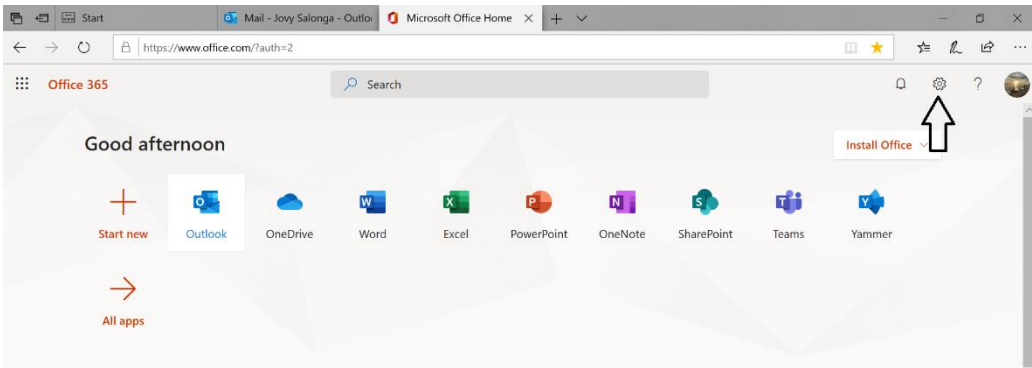


Fig. 8

3. Select “Change your password” . *See Fig 9.*

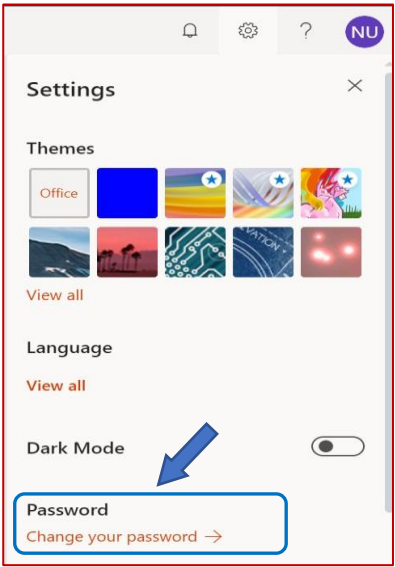
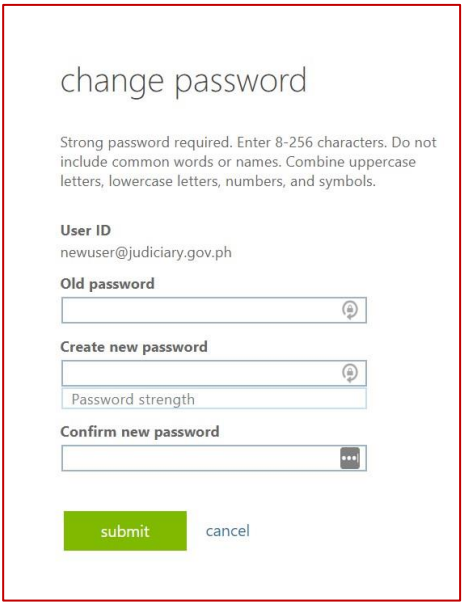


Fig. 9

3. Type your current password, then type a new password and type it again to verify. Click the submit button. **See Fig. 10.**



change password

Strong password required. Enter 8-256 characters. Do not include common words or names. Combine uppercase letters, lowercase letters, numbers, and symbols.

User ID
newuser@judiciary.gov.ph

Old password

Create new password

Password strength

Confirm new password

submit cancel

Fig. 10

Please follow the guidelines below on general recommendations for creating a strong password.

A Strong Password should:

- be at least 8 characters in length
- contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
- have at least one numerical character (e.g. 0-9)
- have at least one special character (e.g. ~!@#\$\$%^&*()_-=)

A Strong Password should not:

- spell a word or series of words that can be found in a standard dictionary
- spell a word with a number added to the beginning and the end
- be based on any personal information such as user id, family name, pet, birthday, etc.

The following are several recommendations for maintaining a Strong Password:

- Do not share your password with anyone for any reason.
- Passwords should not be shared with anyone, including any friends, colleagues or staff.
- Change your password upon indication of compromise. If you suspect someone has compromised your account, change your password immediately. Be sure to change your password from a computer you do not typically use.
- Consider using a passphrase instead of a password. A passphrase is a password made up of a sequence of words with numeric and/or symbolic characters inserted throughout. A passphrase could be a lyric from a song or a favorite quote. Passphrases typically have additional benefits such as being longer and easier to remember. For example, the passphrase “My passw0rd is \$uper str0ng!” is 28 characters long and includes alphabetic, numeric and special characters. It is also relatively easy to remember. It is important to note the placement of numeric and symbolic characters in this example as they prevent multiple words from being found in a standard dictionary. The use of blank spaces also makes a password more difficult to guess.
- Do not write your password down or store it in an insecure manner. As a general rule, you should avoid writing down your password. In cases where it is necessary to write down a password, that password should be stored in a secure location and properly destroyed when no longer needed.
- Do not use automatic logon functionality. Using automatic logon functionality negates much of the value of using a password. If a malicious user is able to gain physical access to a system that has automatic logon configured, he or she will be able to take control of the system and access potentially sensitive information.

ADDITIONAL NOTES:

- Like in any other email systems (i.e. Gmail, Yahoo Mail), the Microsoft Outlook app may be installed in mobile devices in both Android and IOS.
- This guide was created by the MIS Office of the Supreme Court. For queries in using Microsoft Outlook Email, please send them to support.email@judiciary.gov.ph.