FAQs – 2 Factor Authentication (2FA) for Alumni Office365@NTU user accounts

Q1. Why is NTU introducing 2FA?

A1. Increased digital interconnectivity calls for greater personal awareness of cyber security and protection against cyber-threats. 2FA provides that additional layer of security to protect against unauthorised access to NTU services and data. With 2FA, it'll be more difficult for nefarious actors to gain unauthorised access to NTU digital assets. These methods include (1) something you know, that is, your Office365 account username (username@e.ntu.edu.sg) and password, and (2) something you have, that is, the Microsoft Authenticator app configured on your mobile device to authenticate access.

Q2. How do I setup 2FA for the first time and when changing to a new phone?

A2. Click here for detailed step-by-step instructions. When changing to a new phone please register the phone first before discarding the old one. Do remember to also de-register your old phone if it is no longer being used for 2FA.

Q3. What do I need to do if my mobile device registered for 2FA is stolen or lost? Who can I contact if I need help?

A3. First, please submit a request to deactivate the 2FA token on the lost phone. Once you have received a notification from NTU ServiceNow informing you that the old 2FA token has been deactivated, re-setup your 2FA again on your new mobile device.

Q4. I have changed to a new mobile handset or mobile number. How do I update my 2FA details?

A4. Please refer to this guide. Do not wipe off date or dispose your old mobile handset until you have successfully completed the re-enrolment.

Q5. Does 2FA work with international mobile numbers?

A5. Yes, international mobile numbers are supported. Please refer to this guide on how to add or change your mobile numbers. Phone numbers will only be used for account security. Please note that standard telephone and SMS charges will apply.

Q6. Is 2FA required for all the online service platforms I use at NTU?

A6. The 2FA is being rolled out progressively at NTU for Alumni. Office365@NTU will be the first application to implement 2FA from 15 May 2024.

Q7. Will there be charges for the Call Back method and One Time Password method when using 2FA?

A7. The Multi Factor Authentication service by Office365@NTU does not charge users for calls or SMS texts sent. Users may be subject for usage charges to receive calls or SMS texts just like any other call or text based on their personal mobile plan subscriptions they have signed up with their respective Mobile Service Providers.

Q8. Why is it a good idea to have more than one 2FA authentication method configured and ready for my Office365@NTU account?

A8. Though text/SMS One Time Password is supported, we highly recommend the use of the Microsoft Authenticator app. Text/SMS messages have known security flaws making them vulnerable to potential exploitation. By adding Microsoft Authenticator app as a second/backup authentication method, you have another method to authenticate your logon especially when you need to access your Office365@NTU urgently.

Q9. Why is it a good idea to add my personal email address in the security info page?

A9. With your external email address, you will be able to use Microsoft's Self Service Password Reset portal anytime, when you need to reset your **@e.ntu.edu.sg** password. Microsoft will not use your email address for any other purpose.