

PANDUAN

AKTIVASI MULTI-FACTOR AUTHENTICATION

v1.3

Direktorat Pengembangan Teknologi dan Sistem Informasi
Institut Teknologi Sepuluh Nopember

©2023

Deskripsi Panduan

Nama Panduan	: Panduan Aktivasi Multi-Factor Authentication
Tujuan Panduan	: Membantu Civitas Akademika ITS dalam Mengaktifkan metode Multi-Factor Authentication untuk mengakses aplikasi Office 365
Pengguna Panduan	: Mahasiswa, Dosen, dan Tenaga Kependidikan ITS
Penanggung Jawab	: Layanan Teknologi dan Sistem Informasi, DPTSI-ITS



Riwayat Revisi Dokumen

No.	Versi	Tanggal	Deskripsi
1.	1.1	13/11/2023	Dokumen awal Panduan Aktivasi MFA
2.	1.2	20/11/2023	• Menambahkan informasi hal yang perlu disiapkan (hal. 5) • Menambahkan icon petunjuk dimana proses dilakukan (hal. 6) • Menambahkan langkah instalasi Microsoft Authenticator (hal. 8) • Menambahkan informasi baru pada langkah Pengaktifan MFA (hal. 11 dan 12) • Menambahkan gambar baru pada langkah Scan QR a Code (hal. 13) • Menambahkan informasi baru pada langkah Mencoba Microsoft Authenticator (hal. 15)
3.	1.3	08/12/2023	• Menambahkan informasi akses aka.ms/mysecurityinfo (hal. 16) • Menambahkan langkah metode masuk lainnya (metode: email) (hal. 20 , 21 , 22) • Menambahkan langkah metode telepon (hal. 24 , 25 , 26 , 27) • Menambahkan tampilan metode yang sudah didaftarkan (hal. 28)



Apa itu MFA?

MFA atau multi-factor authentication merupakan proses masuk akun yang mengharuskan pengguna memasukkan informasi tambahan selain kata sandi. Seperti menggunakan sidik jari atau memasukkan kode yang dikirim ke nomor telepon.

Apa saja manfaat MFA?

1. Meningkatkan perlindungan keamanan;
2. Menghindari aksi peretasan ke aplikasi dan akses sumber daya yang memanfaatkan login dengan user ID, email, dan password;
3. Melindungi data pengguna dari pencurian kredensial.



Hal yang perlu disiapkan:

1. Smartphone dengan nomor seluler aktif dan dapat menerima SMS;
2. Aplikasi Microsoft Authenticator atau autentikator lain jika sudah menggunakan sebelumnya;
3. Laptop/komputer.



Petunjuk:



Proses terjadi di hp



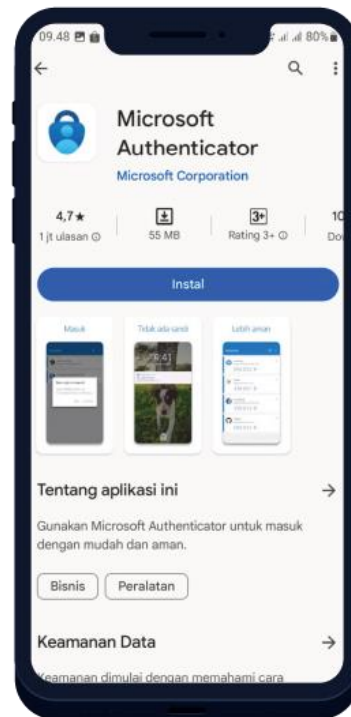
Proses terjadi di laptop



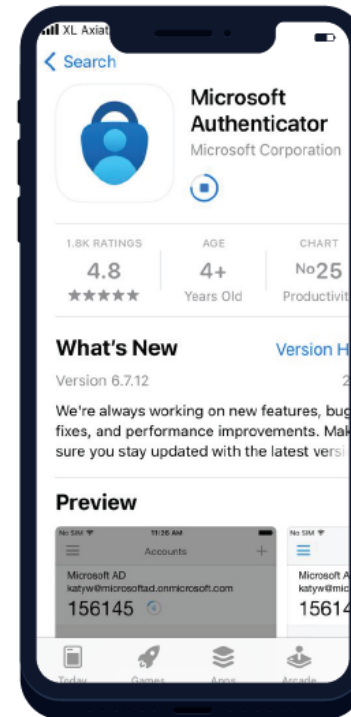
1. Instalasi Aplikasi Microsoft Authenticator

Sebelum melakukan aktivasi, pengguna disarankan mengunduh aplikasi **Microsoft Authenticator** melalui PlayStore/AppStore.

Tampilan PlayStore



Tampilan AppStore



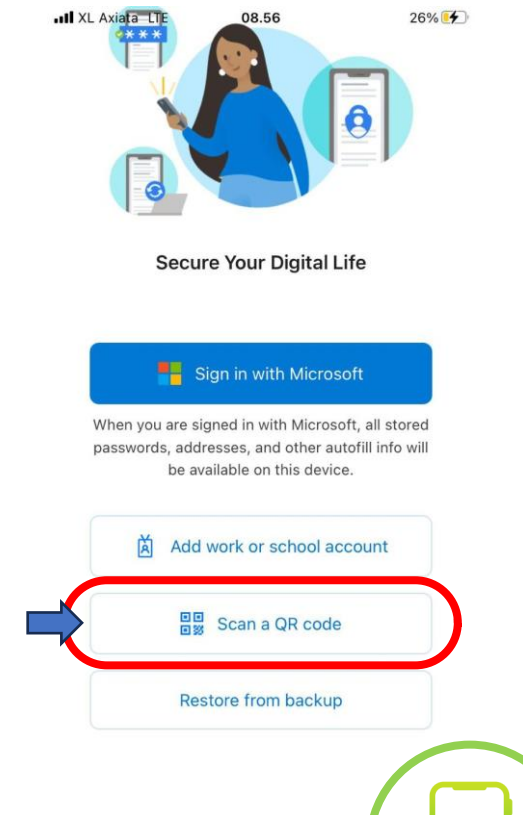
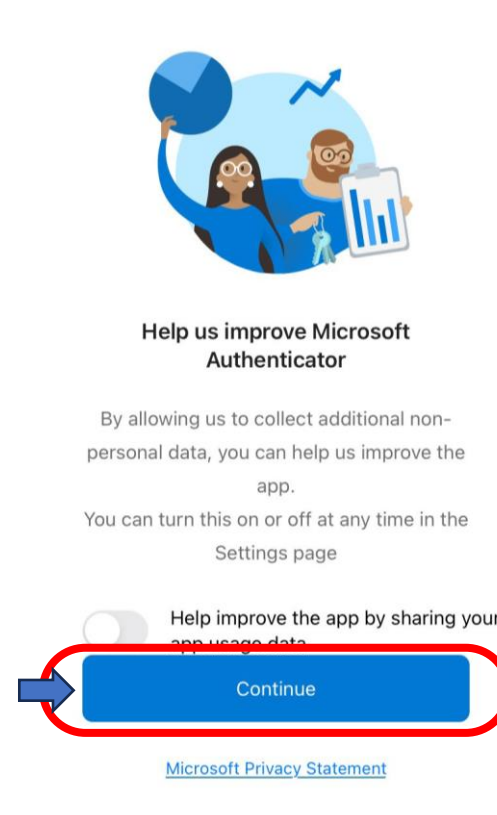
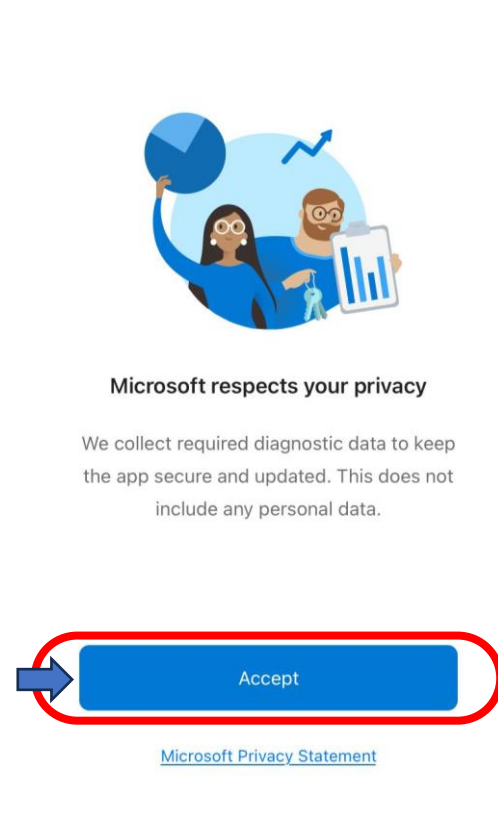
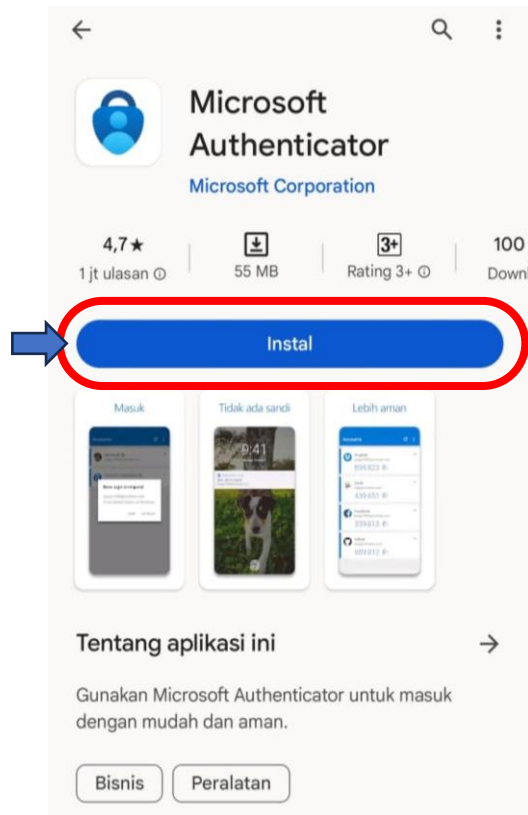
Langkah instalasi Microsoft Authenticator:

1. Klik tombol **Install**.

2. Klik tombol **Accept**.

3. Klik tombol **Continue**.

4. Klik **Scan a QR code**.



Siapkan laptop Anda dan buka link berikut: <https://aka.ms/mfasetup>



2. Sign in ke <https://aka.ms/mfasetup>

Setelah masuk ke halaman <https://aka.ms/mfasetup>.

Sign in menggunakan email ITS dan password myITS (klik Enter/Masuk).
Lalu klik tombol Selanjutnya/Next.



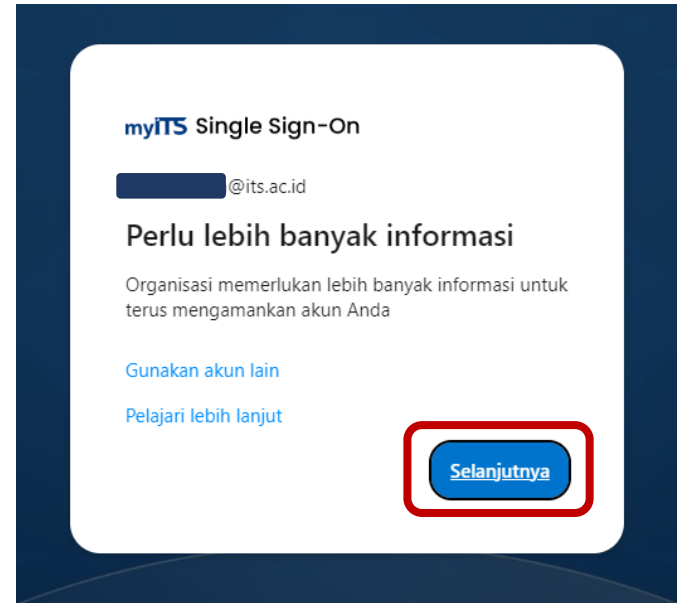
myITS Single Sign-On

← [redacted]@its.ac.id

Masukkan sandi

[redacted]

Masuk



myITS Single Sign-On

[redacted]@its.ac.id

Perlu lebih banyak informasi

Organisasi memerlukan lebih banyak informasi untuk terus mengamankan akun Anda

[Gunakan akun lain](#)

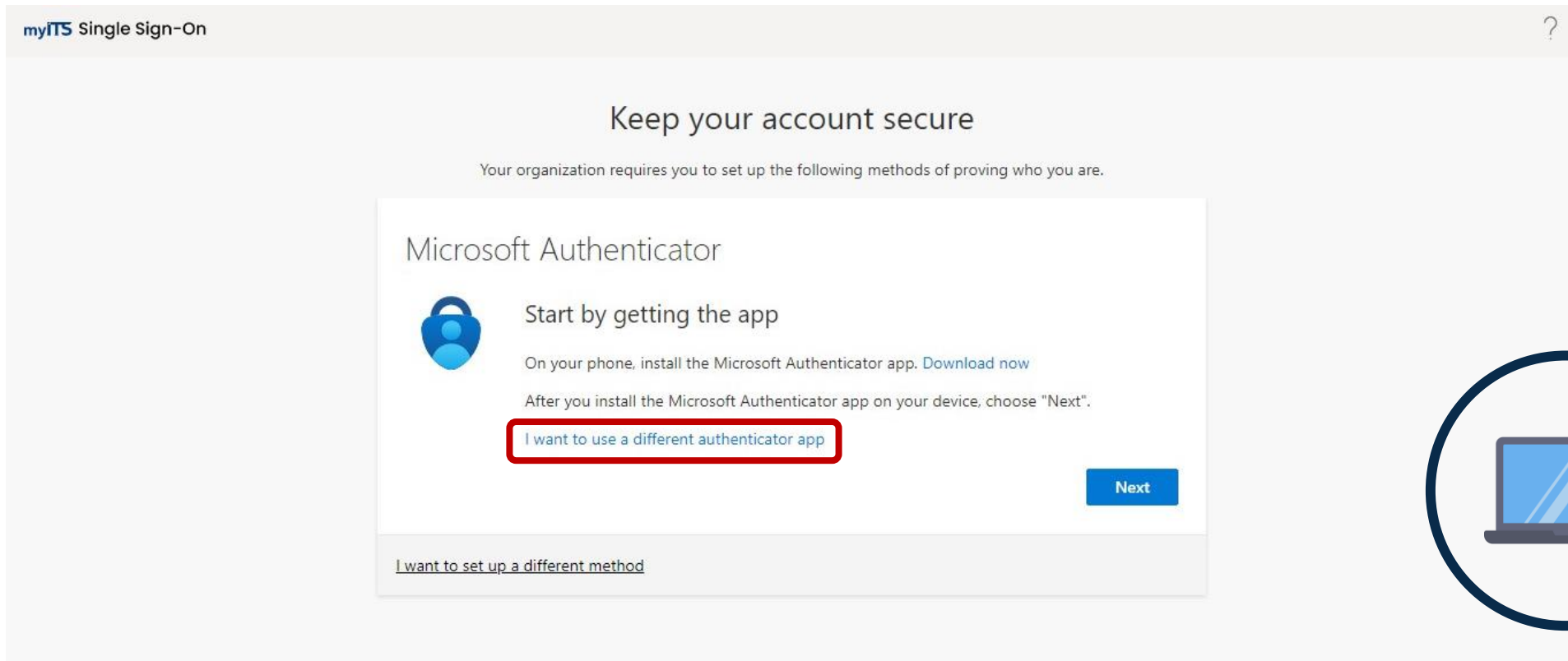
[Pelajari lebih lanjut](#)

Selanjutnya



3. Mulai ke Langkah Pengaktifan MFA

Klik **I want to use a different authenticator app**. Lalu klik Next/Berikutnya.



4. Lanjutan

Klik tombol **Next/Berikutnya**.

Authenticator app



Set up your account

In your app, add a new account.

Back

Next



5. Scan a QR code

Nantinya **akan muncul QR code**. Siapkan hp Anda untuk melakukan Scan a QR code yang ada di laptop Anda. Klik tombol **Next/Berikutnya**.

Authenticator app

Scan the QR code

Use the authenticator app to scan the QR code. This will connect your authenticator app with your account.

After you scan the QR code, choose "Next".



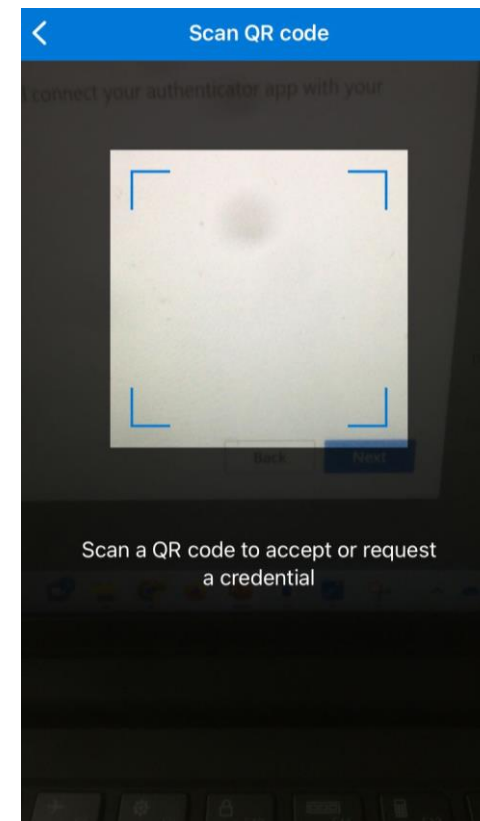
Can't scan image?



Scan QR code

Back

Next



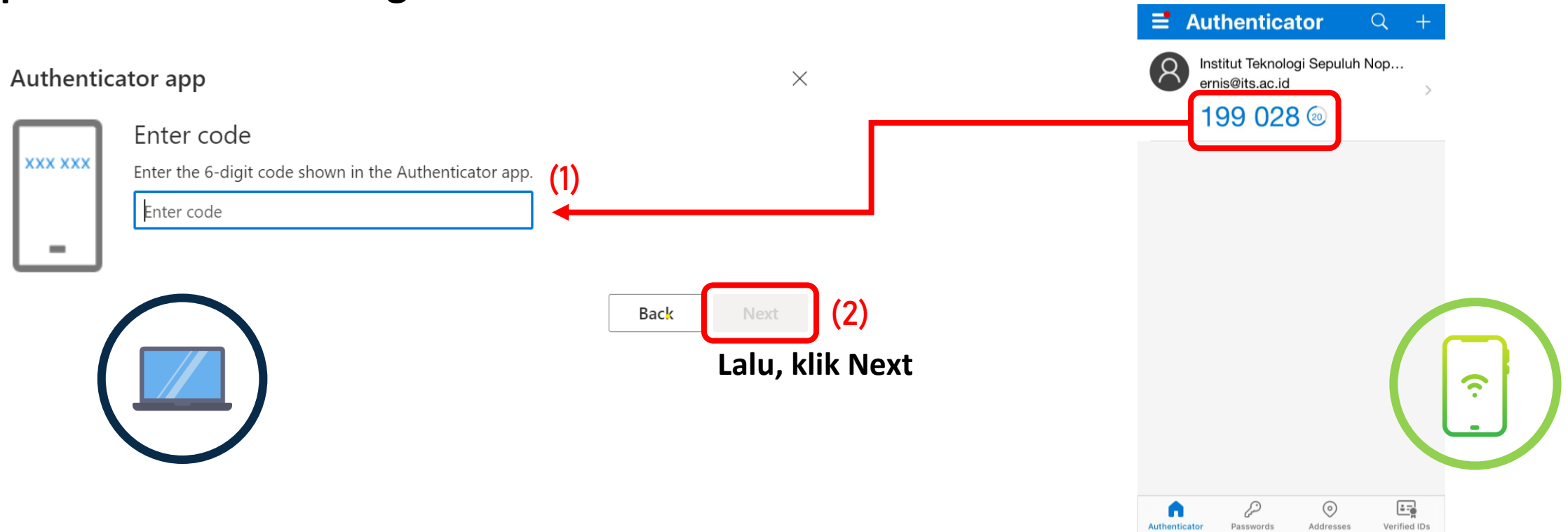
6. Mencoba Microsoft Authenticator

Masukkan angka/code yang tertera di tampilan layar laptop Anda ke aplikasi Microsoft Authenticator di hp Anda, lalu klik tombol **Berikutnya/Next**.



Beberapa pengguna mungkin ada yang diminta memasukkan kode dari hp ke web.

Jika perintah yang diberikan adalah memasukkan kode dari aplikasi autentikator, maka buka aplikasi autentikator Anda, dan masukkan kode yang tertera di aplikasi ke kotak dialog berikut:



7. Akses <https://aka.ms/mysecurityinfo>

Masuk ke halaman <https://aka.ms/mysecurityinfo> untuk menambahkan metode masuk lainnya.

Sign in menggunakan email ITS dan password myITS (klik Enter/Masuk). Lalu klik tombol Selanjutnya/Next.



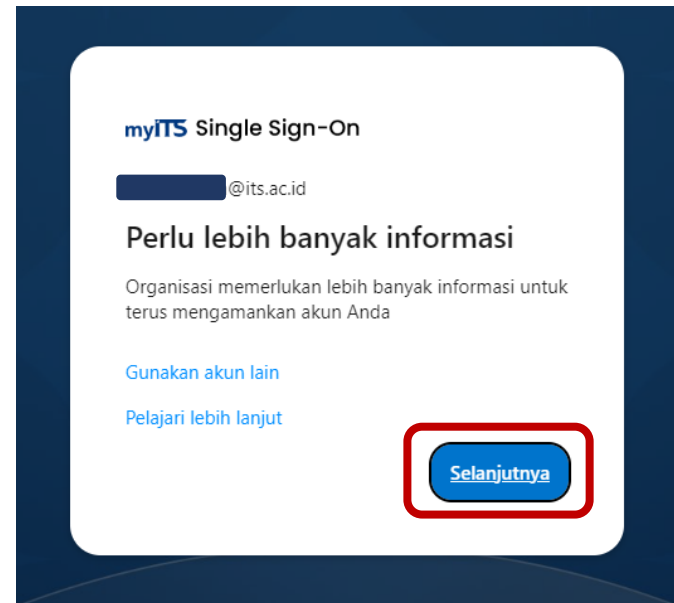
myITS Single Sign-On

← [redacted]@its.ac.id

Masukkan sandi

Sandi

Masuk



myITS Single Sign-On

[redacted]@its.ac.id

Perlu lebih banyak informasi

Organisasi memerlukan lebih banyak informasi untuk terus mengamankan akun Anda

[Gunakan akun lain](#)

[Pelajari lebih lanjut](#)

Selanjutnya



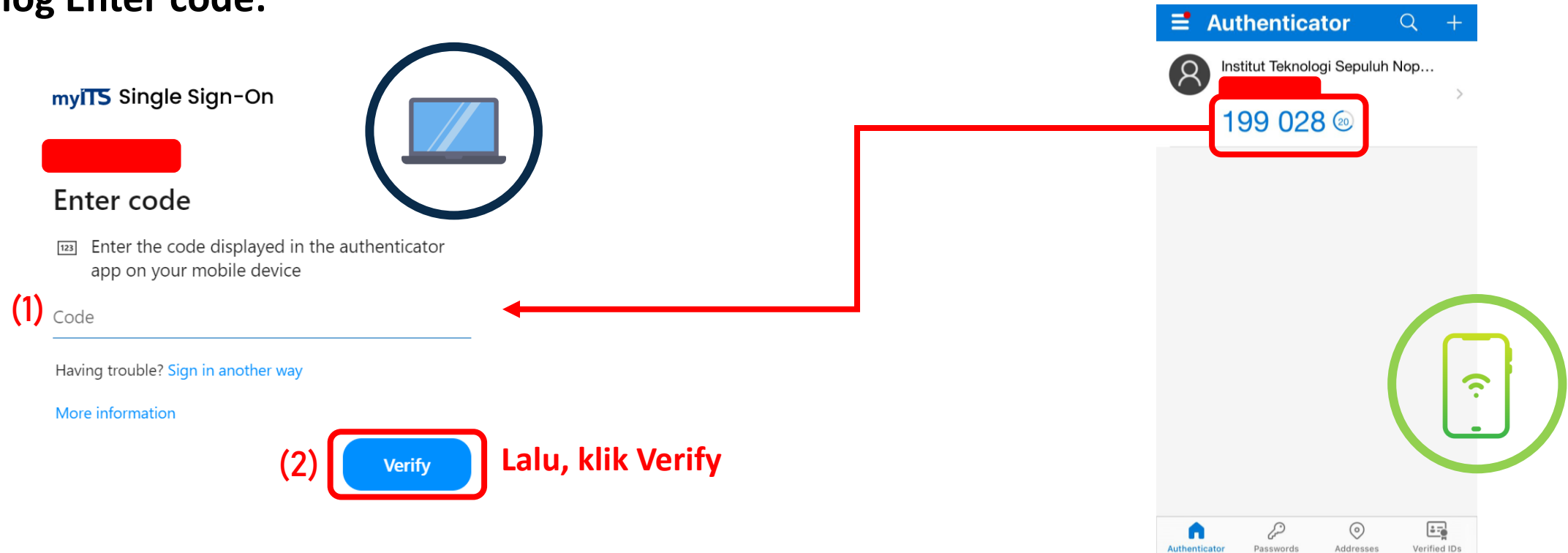
8. Ketika melanjutkan sign in, Anda akan diminta memasukkan kode verifikasi.

Masukkan kode yang muncul di web ke aplikasi Microsoft Authenticator di hp Anda.



Beberapa pengguna mungkin ada yang diminta memasukkan kode dari aplikasi autentikator ke web.

Jika perintah yang diberikan adalah memasukkan kode dari aplikasi autentikator, **maka buka aplikasi autentikator Anda, dan masukkan kode yang tertera di aplikasi ke kotak dialog Enter code:**



9. Klik Yes di kotak dialog Stay signed in jika menggunakan laptop pribadi

myITS Single Sign-On

@its.ac.id

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

☐ Don't show this again

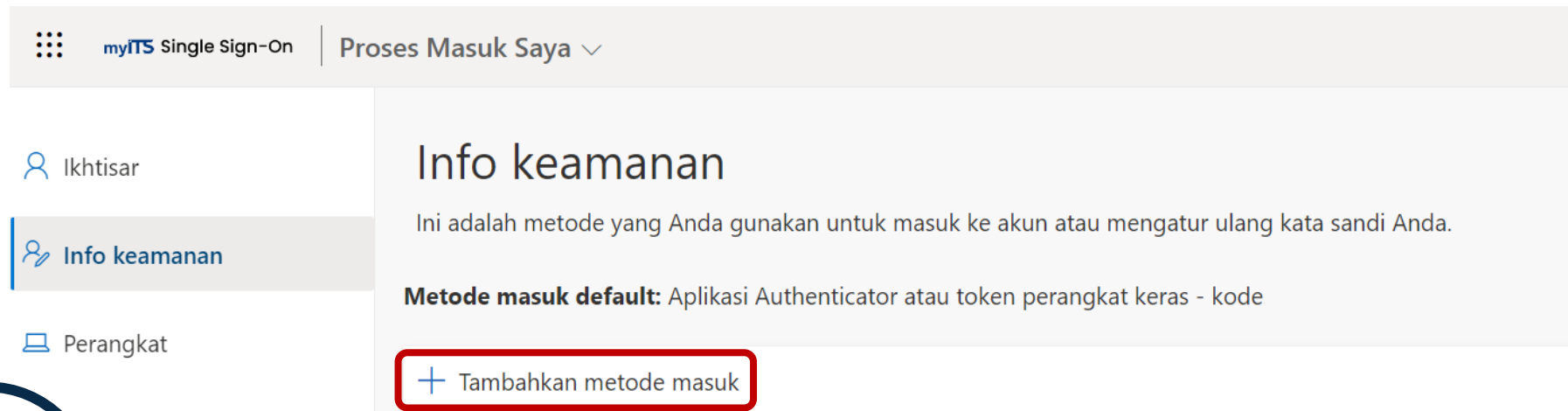
No

Yes



10. Menambahkan metode masuk

Setelah masuk ke halaman aka.ms/mysecurityinfo, klik tombol **Tambahkan metode masuk/Add sign-in method**.

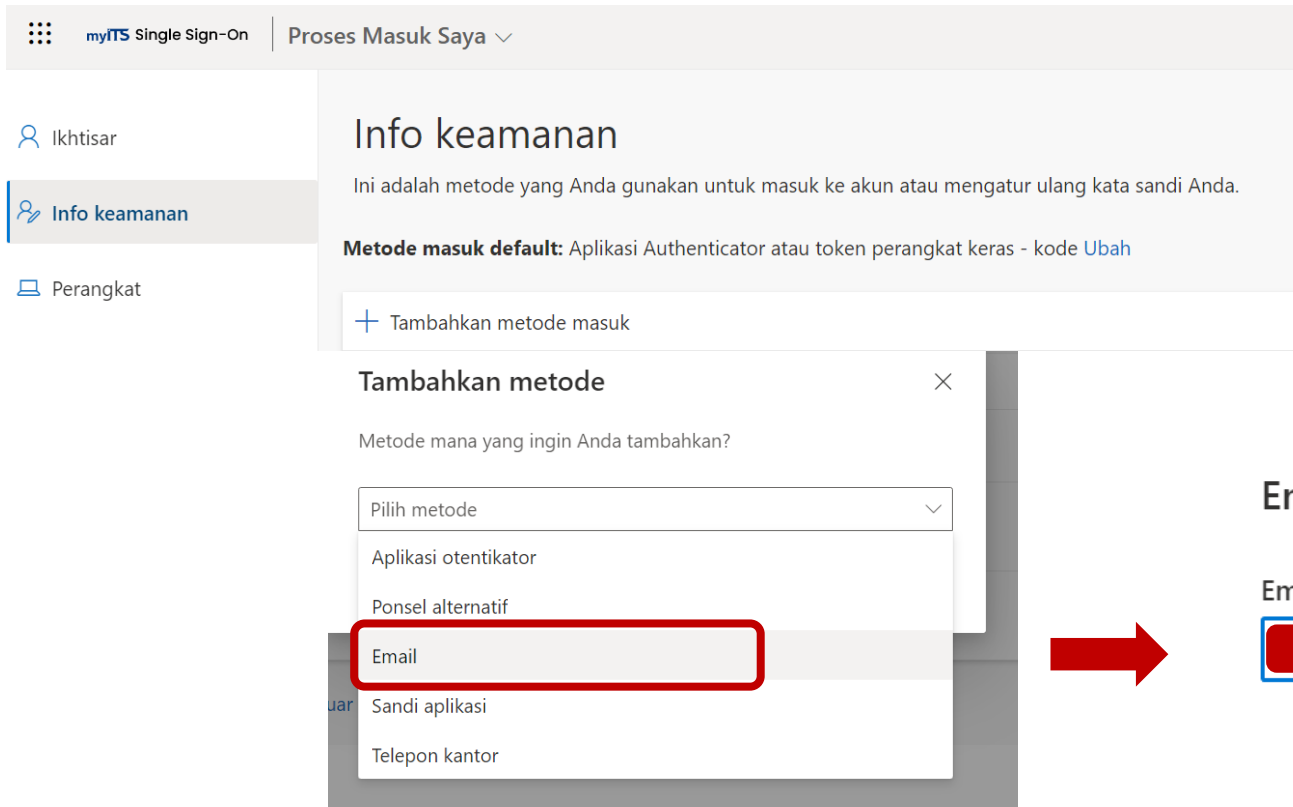


Klik tambahkan metode masuk.



11. Menambahkan metode Email

Pilih metode **Email**. Isi email alternatif Anda (selain email ITS). Klik Next/Berikutnya.



myITS Single Sign-On | Proses Masuk Saya

Ikhtisar

Info keamanan

Perangkat

Info keamanan

Ini adalah metode yang Anda gunakan untuk masuk ke akun atau mengatur ulang kata sandi Anda.

Metode masuk default: Aplikasi Authenticator atau token perangkat keras - kode [Ubah](#)

+ Tambahkan metode masuk

Tambahkan metode

Metode mana yang ingin Anda tambahkan?

Pilih metode

- Aplikasi otentikator
- Ponsel alternatif
- Email**
- Sandi aplikasi
- Telepon kantor



Email

Email apa yang ingin Anda gunakan?

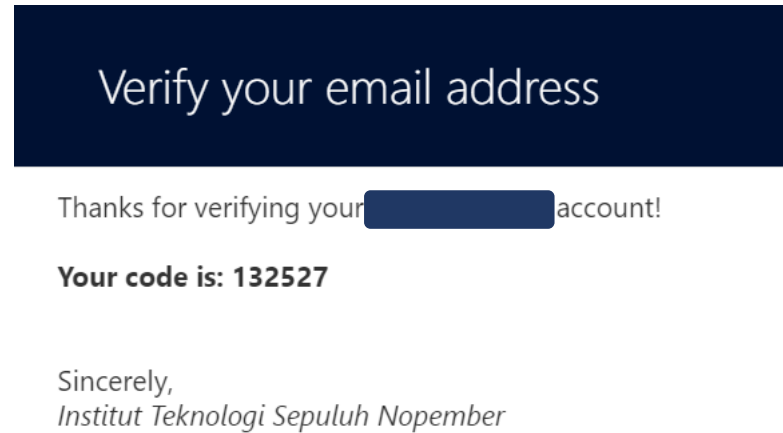
Batal

Berikutnya



12 Masukkan Kode dari Email

Masukkan kode yang masuk ke email Anda.



Email



Kami baru saja mengirim kode ke [redacted]@gmail.com

Masukkan kode

[Kirim ulang kode](#)

Kembali

Berikutnya

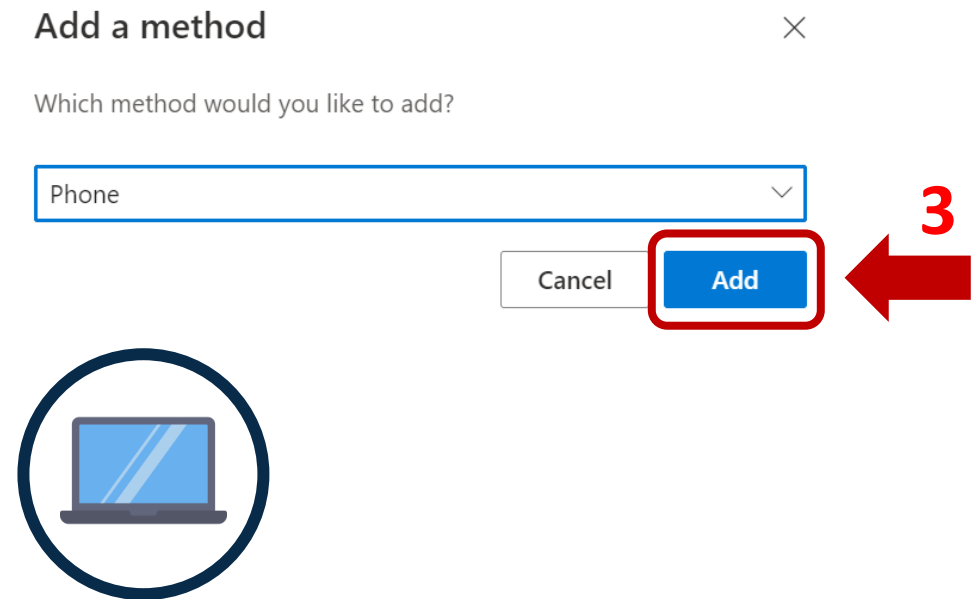
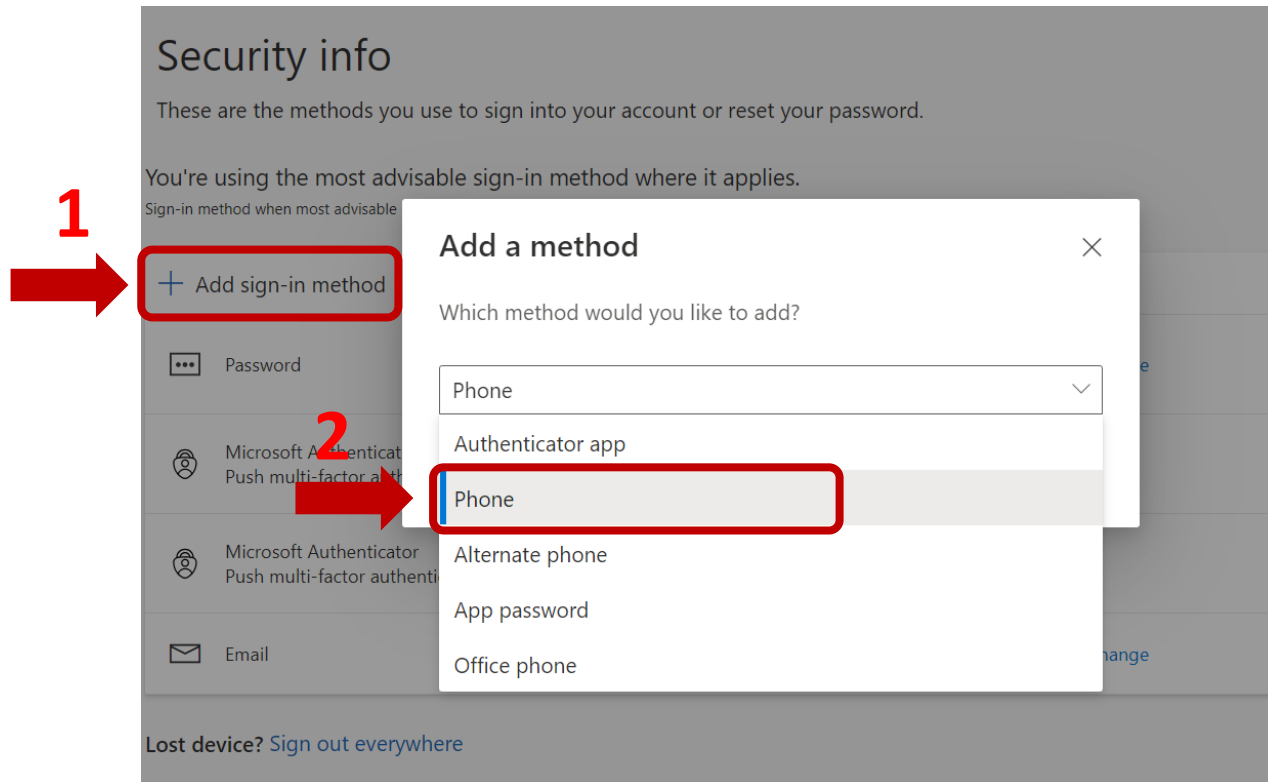


Menambahkan metode lain: metode telepon



13. Menambahkan metode Telepon

Pilih **Add sign-in method/Tambahkan metode masuk** dan pilih metode **Phone/Telepon**.
Lalu klik Add.



14. Pilih kode negara dan masukkan nomor telepon

Phone



You can prove who you are by answering a call on your phone or receiving a code on your phone.

What phone number would you like to use?

Indonesia (+62) 

☒ Receive a code

☐ Call me

Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#).



Cancel

Next

Pilih kode negara +62 dan masukkan nomor telepon.

Lalu pilih **Receive a code/Kirimkan kode kepada saya** untuk menerima kode melalui SMS.

Setelah semua kolom terisi, klik Next/Berikutnya.



15. Masukkan Captcha

Ketikkan captcha yang muncul. Lalu klik Next/Berikutnya.

Phone

Please show you are not a robot.



VySPLX6R

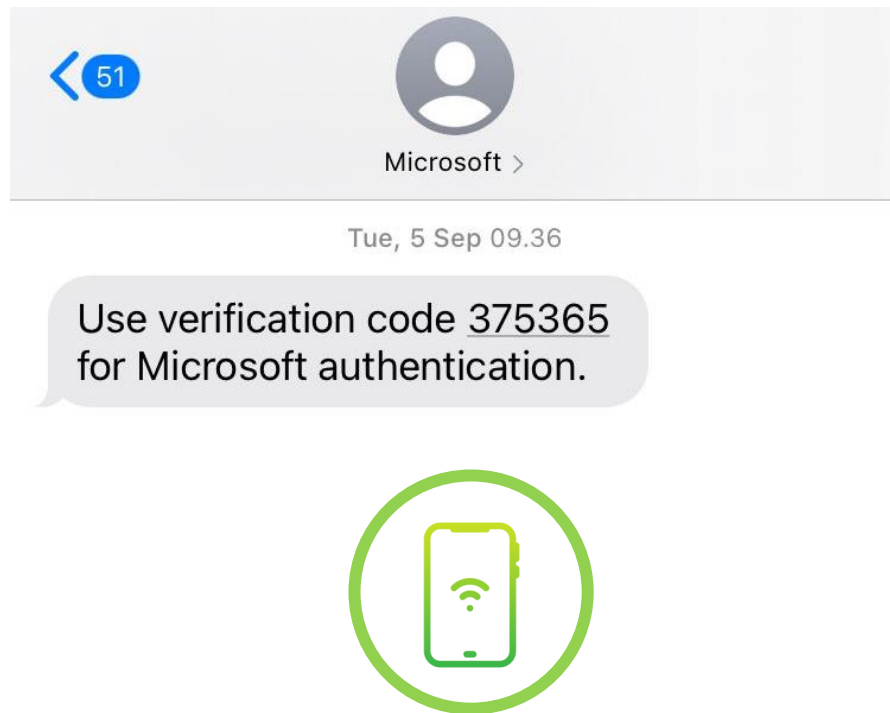
Back

Next



16. Lihat pesan yang masuk ke nomor hp Anda

Jika Anda memilih **Kirimkan kode kepada saya/Text me a code**, pesan yang berisi kode verifikasi akan terkirim ke nomor hp Anda. **Masukkan kode yang diterima ke kotak dialog Enter code** dan klik **Next/Berikutnya**.

A screenshot of a mobile app screen titled 'Phone' with a close button (X) in the top right. The text says: 'We just sent a 6 digit code to +62 [redacted] Enter the code below.' There is an input field labeled 'Enter code' and a blue link 'Resend code' below it. At the bottom right are two buttons: 'Back' and 'Next'. Below the screen is a dark blue circular icon containing a laptop.

17. Tampilan metode yang sudah didaftarkan

Metode yang sudah didaftarkan akan muncul dalam tampilan halaman Security Info/Info Keamanan.

Security info

These are the methods you use to sign into your account or reset your password.

You're using the most advisable sign-in method where it applies.
Sign-in method when most advisable is unavailable: Authenticator app or hardware token - code [Change](#)

+ Add sign-in method

 Phone		Change	Delete
 Password	Last updated: 2 months ago	Change	
 Authenticator app Time-based one-time password (TOTP)			Delete
 Authenticator app Time-based one-time password (TOTP)			Delete
 Email		Change	Delete



ADVANCING
HUMANITY



Kampus
Merdeka
INDONESIA JAYA

Silahkan klik link di bawah ini untuk
informasi lebih lanjut:

servicedesk.its.ac.id

TERIMA KASIH

Direktorat Pengembangan Teknologi dan Sistem Informasi
Institut Teknologi Sepuluh Nopember

©2023