UNIVERSITAS YARSI

14/08/2020

Tantangan Keamanan Siber

Ahmad Sabiq

Dosen Teknik Informatika Universitas YARSI

https://www.yarsi.ac.id/

registrar@yarsi.ac.id

@universitasyarsi

YARSI TV

https://www.facebook.com/universitas.yarsi.1/

Menara YARSI Kavling 13
Jl. Let. Jend. Suprapto
Cempaka Putih, Jakarta Pusat
DKI Jakarta, Indonesia 10510

UNIVERSITAS YARSI

Menara YARSI Kav. 13
Jl. Let. Jend. Suprapto
Cempaka Putih, Jakarta Pusat
DKI Jakarta. Indonesia 10510

https://www.yarsi.ac.id/
registrar@yarsi.ac.id
@universitasyarsi
YARSI TV

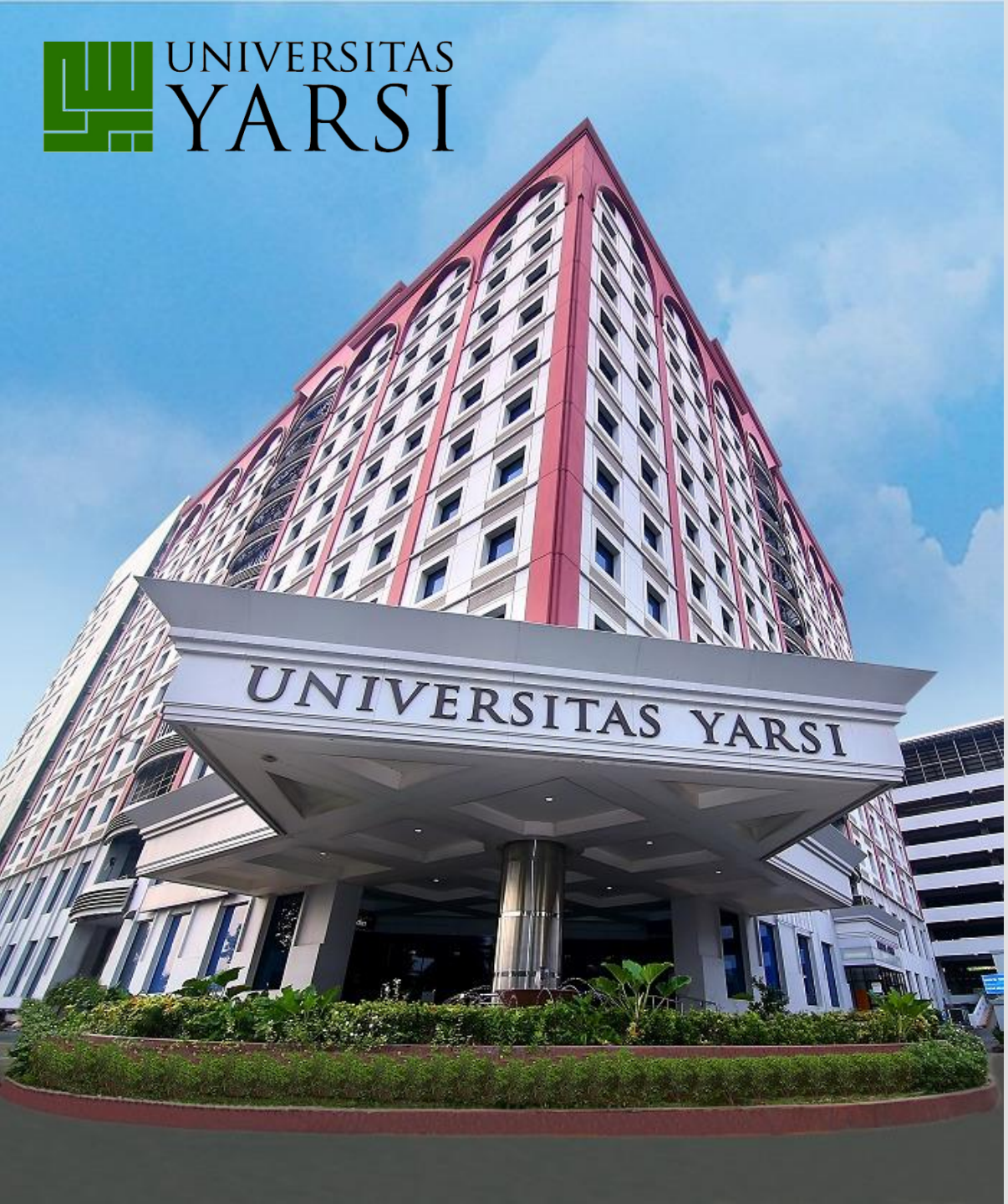
https://www.facebook.com/universitas.yarsi.1/

Fakultas dan Program Studi

1. Fakultas Kedokteran
   Program Studi Pendidikan dan Profesi
2. Fakultas Kedokteran Gigi
   Program Studi Pendidikan & Profesi
3. Fakultas Teknologi Informasi
   Program Studi Teknik Informatika & Perpustakaan dan Science Informasi
4. Fakultas Ekonomi dan Bisnis
   Program Studi Akutansi & Manajemen
5. Fakultas Hukum
   Program Studi Ilmu Hukum
6. Fakultas Psikologi
   Program Studi Psikologi
7. Sekolah Pascasarjana
   Program Studi Manajemen, Biomedis, & Kenotariatan

Pusat Penelitian

1. Genetik/Genomik
2. E-Health
3. Studi Halal
4. Studi Sel Punca
5. Studi Herbal
6. Studi Telomer



Lisensi Penggunaan

BY-NC-SA

Rapat selama WfH

Apakah Zoom aman?

Cyber Security ?

- Memproteksi diri sendiri dan/atau yang lain dari serangan, tertutama menggunakan komputer

- Perlindungan / proteksi / Keamanan informasi yang bersifat digital.
  - Saat informasi:
    - disimpan
    - ditransfer
    - digunakan

Tujuan porteksi & keamanan informasi (CIA Triad)

Confidentiality

- Informasi tidak diketahui oleh pihak lain yang tdk berkepentingan

Integrity

- Informasi tidak berubah / utuh apa adanya / tidak ada perubahan.

Availibility

- Informasi tersedia ketika diakses oleh pengguna (yang semestinya)
  - Jika saat ada transaksi server data mati maka tidak akan terjadi transaksi

Ruang lingkup Cyber Security

- User
- Organisasi
- Profider
- Penyedia Infrastruktur
- Pemerintah

Tantangan Cyber Security

- Hampir setengah penduduk dunia terhubung ke internet
- Tahun 2018 pengguna internet berjumlah 95,2 juta
- Lebih dari 15 miliar perangkat terhubung ke internet

- **Semakin banyak sasaran yang bisa diserang**

Mat Honan's Epic Hacking

- Agustus 2012, peretas menghapus semua data Mat Honan di iPhone, iPad, dan Mac Book.
  - Foto-foto anak bayinya dan keluarga, serta salinan digital datanya dihapus semua.
- Akun Twitter juga diretas.
  - Mentwit pesan-pesan rasis.
- Akun Google dihapus.
  - Berisi email-email penting selama delapan tahun.
    - *two-factor authentication* tidak diaktifkan

https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

Mat Honan’s Epic Hacking

- Bagaimana peretas melakukan serangan ini?
  - yang secara pribadi sangat menghancurkan memebuatnya tampak memalukan?

- **Ternyata**
- Serangan dilakukan tanpa perlu menulis sebaris kode program apapun untuk menyerang.
- Penyerang tidak memerlukan program komputer khusus, juga tidak membutuhkan keterampilan teknis yang sangat mengesankan.
- browser web, telepon, dan **informasi pribadi tentang honan yang tersedia** untuk siapa saja yang memiliki koneksi internet.

https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

Mat Honan’s Epic Hacking

- **Bagaimana peretas mendapatkan akun amazon?**

- Para peretas memulai dengan mengumpulkan semua informasi pribadi tentang honan yang dapat mereka kumpulkan dari akun media sosial Honan dan catatan publik online.
- mereka mendapat alamat email honan, alamat fisik, dan bit informasi lainnya, dan mereka menggunakan informasi itu untuk memecahkan akun amazon Honan.

https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

Mat Honan's Epic Hacking

- **Bagaimana peretas mendapatkan akun amazon?**

- Para peretas menelepon amazon, berpura-pura menjadi Honan, dan meminta perwakilan amazon untuk mereset ulang akun Honan untuk mereka.
- Peretas menggunakan informasi pribadi Honan – dan juga menggunakan nomor kartu kredit palsu - untuk meyakinkan customer service amazon bahwa peretas adalah benar-benar Mat Honan.

https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

Mat Honan’s Epic Hacking

- **Bagaimana peretas mendapatkan akun Apple?**

- Setelah mengakses akun Amazon Honan, para peretas mengumpulkan informasi pribadi Honan.
- Peretas mendapatkan informasi empat digit terakhir dari nomer kartu kredit Honan.
  - Informasi ini digunakan untuk men-*crack* Apple ID Honan.

https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

Mat Honan’s Epic Hacking

- **Bagaimana peretas mendapatkan akun Apple?**

- Para peretas menggunakan trik yang sama sebelumnya.
- Peretas menelepon customer service dan menggunakan informasi pribadi untuk meyakinkan cs untuk mereset Apple ID Honan untuk peretas.

https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

Mat Honan's Epic Hacking

- **Bagaimana peretas mendapatkan akun Google?**

- Setelah mendapatkan akun Apple, peretas dapat dengan mereset akun Google dan masuk ke akun Google.
- Dari akun google peretas mendapatkan informasi untuk login ke akun twitter, untuk mengirimkan pesan yang sifatnya menyerang dan memalukan.

https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

Mat Honan's Epic Hacking

- **Bagaimana peretas menghapus akun Honan?**

- Untuk menghapus jejak peretas, mereka menghapus akun Google Honan.
- Dengan Apple ID mereka me-*request* penghapusan data jarak jauh untuk macbook, iphone dan ipadnya.
  - Ironisnya ini adalah layanan yang ditujukan untuk melindungi data dari pencurian.

https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

Jika kita berada pada posisi kasus honan

bagaiana cara kita menurunkan resiko pada keamanan akun kita?

Mengurangi Kerentanan Keamanan

- Mengaktifkan otentikasi dua faktor (two-factor authentication) di akun google-nya.
- Mengurangi ancaman atau kemungkinan diserang.
  - Honan lebih mungkin diserang dibanding anda.
  - **Dia adalah penulis artikel tentang *cyber security*.**
- Semakin banyak keuntungan yang didapat dari menyerang Anda, semakin besar kemungkinan Anda akan diserang.
  - target yang menguntungkan, ancamannya meningkat, yang berarti risiko keamanan semakin tinggi.

Mengurangi Risiko Keamanan

- Menurunkan resiko dari serangan peretasan,
  - dengan cara menurunkan dampak dari serangan.
- Contoh, serangan honan berdampak kecil jika honan mem*backup* semua fotonya di disk atau eksternal hd.
- Jika ada backup, semua data dengan mudah dapat direcover.

Berapa banyak akun dan perangkat anda yang dilindungi *password*?

- Email pribadi
- Email pribadi kedua
- Email kantor / kampus
- Media sosial 1
- Media sosial 2
- Media sosial 3
- Media sosial 4
- Blog
- Video streaming 1
- Video streaming 2
- Video streaming 3
- Jaringan rumah
- Layanan musik 1
- Layanan musik 2
- Layanan pajak
- Shoping online
- Lapak online
- Toko online
- Toko online lagi
- Laptop
- Komputer kantor
- Perangkat mobile 1
- Perangkat mobile 2
- Online Banking 1
- Online Banking 2
- Website berita
- E-learning
- sisakad
- dll

10 jenis serangan password

- Diungkapkan pemiliknya
- Social engineering
- Phising
- Key logging
- Wireless sniffing
- Brute force guessing
- Dictionary attacks
- File password tidak dienkripsi
- Password dengan hash value yang diketahui.
- Security questions

Gunakan Password yang KUAT

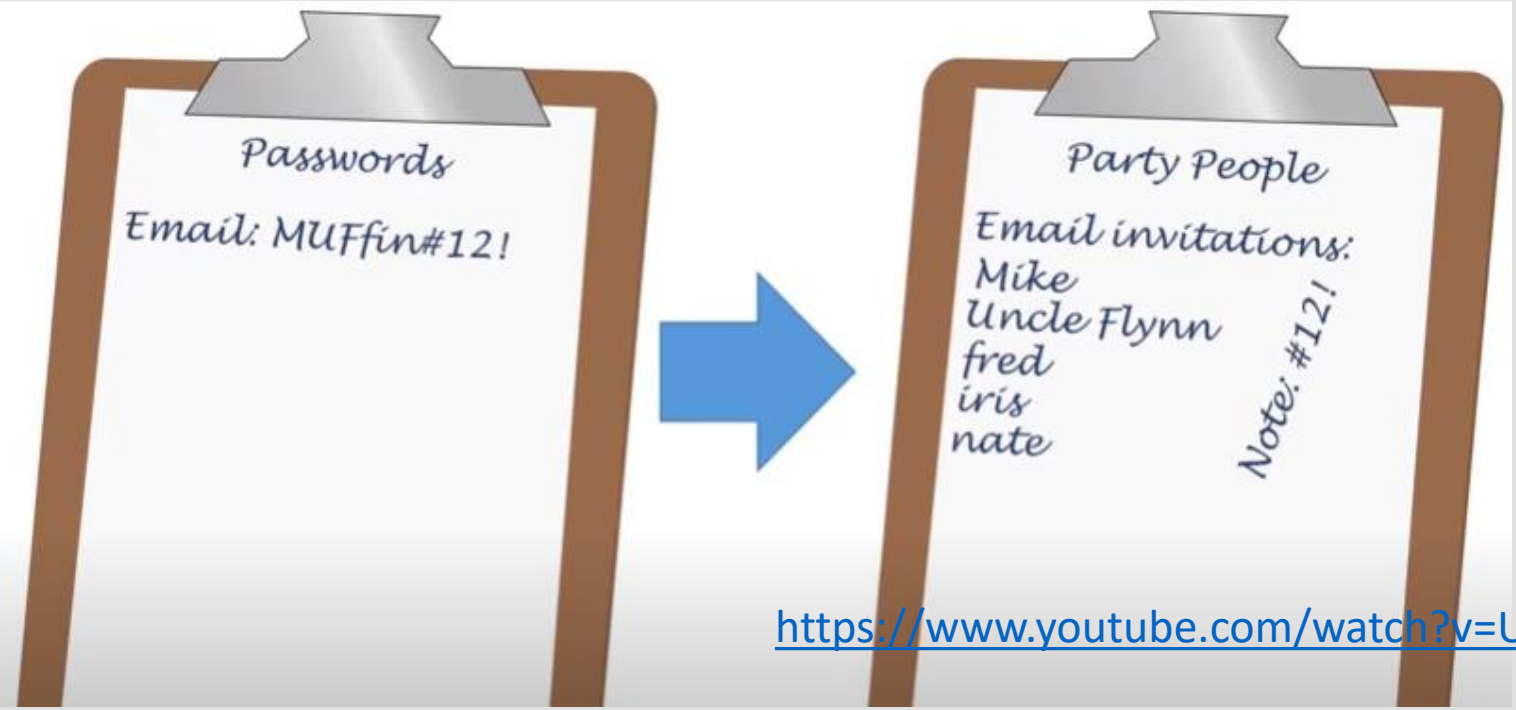
JANGAN !!	HARUS
• Menggunakan nama / kata / angka yang terkait dengan diri kita • Kata yang ada dalam kamus • Kata yang umum digunakan untuk password • Terlalu pendek	• Password dengan gabungan huruf kecil dan kapital, angka dan simbol • Password yang berbeda (*unique*) untuk setiap akun / *device*. • Ganti password dengan teratur. • Tidak pernah menulis password. • Gunakan *multi-factor authentication.*

Tips Mengelola Paswords

Posbindu Goes to Campus

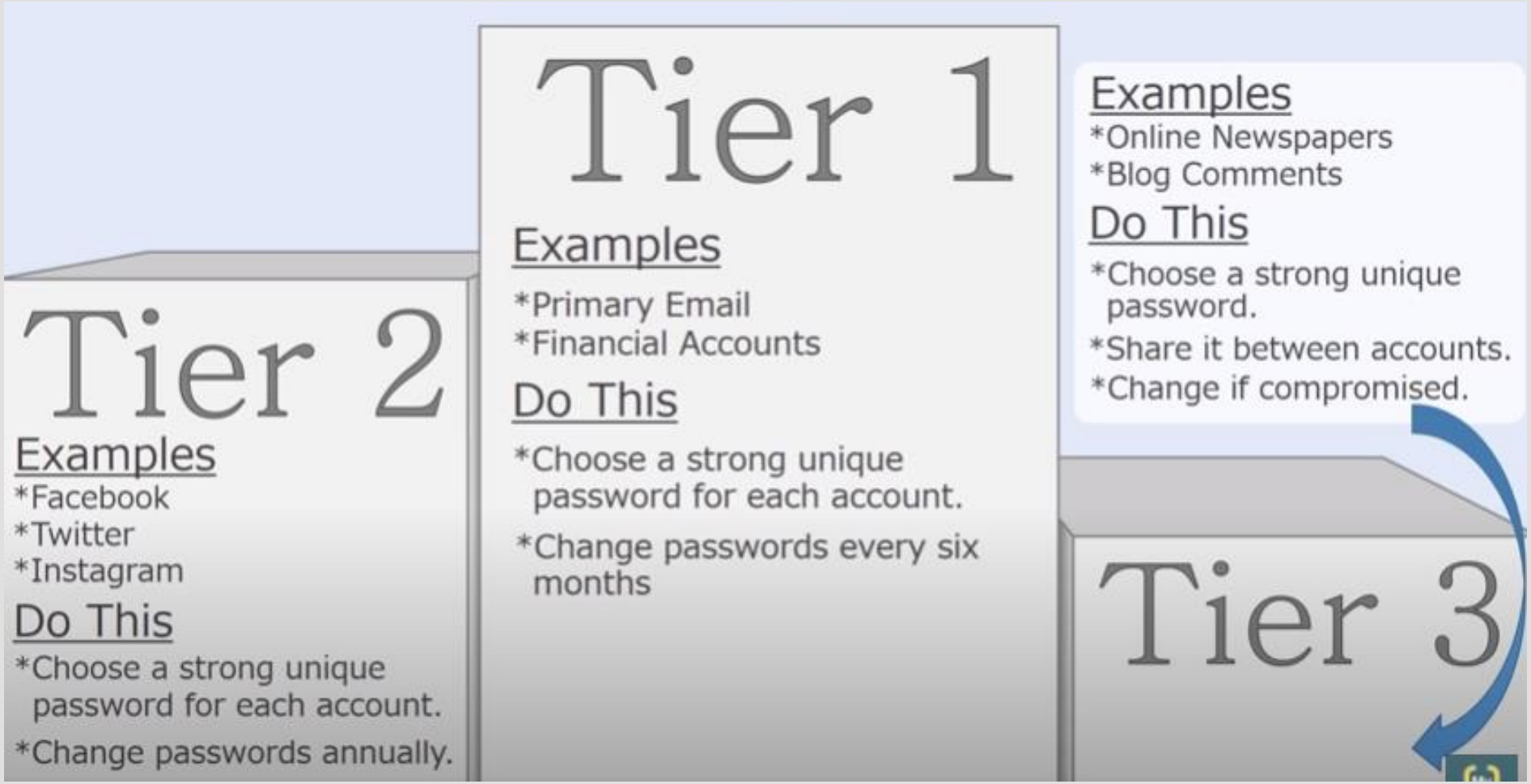
~~Mencatat~~ dengan cara yang aman

- Buat catatan dalam bentuk clue,
- tanpa menulis password, dan jenis akun/perangkat.



https://www.youtube.com/watch?v=U_P23SqJaDc&t=7209s

Buat Tingkatan Akun



https://www.youtube.com/watch?v=U_P23SqJaDc&t=7209s

Gunakan Software Pengelola Password

- Satu Password master
  - LastPass Password Manager
  - Dashlane password manager
  - Keeper
  - dll

UNIVERSITAS YARSI

Terima Kasih

Menara YARSI Kav. 13
Jl. Let. Jend. Suprapto
Cempaka Putih, Jakarta Pusat
DKI Jakarta. Indonesia 10510

https://www.yarsi.ac.id/
registrar@yarsi.ac.id
@universitasyarsi
YARSI TV

https://www.facebook.com/universitas.yarsi.1/

Content Creators

Ahmad Sabiq

Slide Template Designers

Andreas Febrian, Cesario Auditya Pratama, Raihan Ramadhan Yusuf, Reynaldi Pratama

Slide Modificators