

Pengetahuan dan Tips Keamanan Siber dalam  
Menghadapi Kemajuan Teknologi Informasi:

## **Password, MFA, Cryptocurrency, dan AI**

Rifqi Ardia Ramadhan



True Blue Team Fighter

Certification:

ECIH, CHFI, Malware Analysis Path Letsdefend.io

Experience:

- Security Engineer @ Blibli.com
- Technical Consultant Analyst @ MII

Achievements:

- 1<sup>st</sup> Place KKST TNI-AD 2020
- 1<sup>st</sup> Place Hacktrange Independence Day 2023
- 5<sup>th</sup> Place Global Cyberpeace Challenge

---

**Rifqi Ardia Ramadhan**



# What I do

## Blue teaming activities

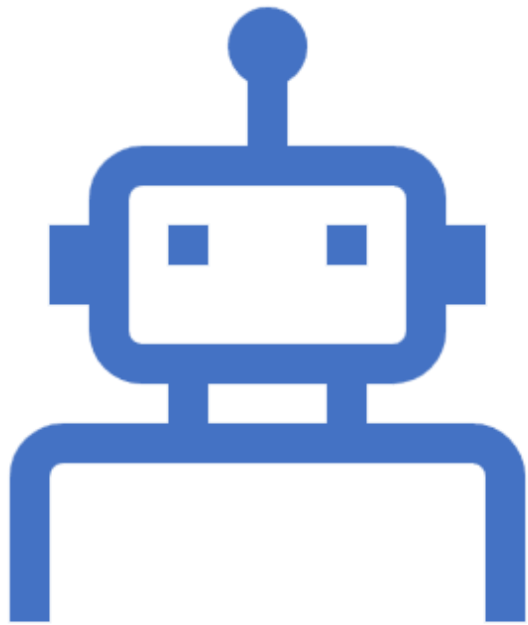
- Digital Forensic and Incident Response
- Security Operations
- Malware Analysis
- SIEM engineering
- Training

## Non-work activities

- CDEF contributor
- Overseer for HCS
- Volatility3 plugin developer

# Membuat Password

Membangun password yang aman untuk semua akun online kalian



# Password

- Password atau Kata Sandi adalah salah satu cara untuk melakukan autentikasi ke aplikasi atau layanan digital
- Hal ini diterapkan untuk memastikan bahwa yang masuk ke aplikasi tersebut adalah orang yang berhak mengakses aplikasi tersebut
- Ada berapa password yang rekan-rekan miliki?  
2? 5? 10?

# Password per Person



Dari survey yang dilakukan NordPass pada tahun 2024, saat ini setiap orang perlu menghafal 87 password untuk berbagai akun bisnis yang dimiliki.



Jika ditotal dengan password untuk akun pribadi, jumlah password rata-rata yang dimiliki user adalah 255!



Angka ini termasuk ke layanan-layanan yang user sudah tidak menggunakannya lagi tapi akunnya tidak ditutup.



Penyebab utamanya diduga berasal dari banyak pekerjaan remote dan digitalisasi berbagai hal, dari pesan antar, belanja, hingga birokrasi.

PASSWORD MEMILIKI  
STANDAR INTERNASIONAL  
YANG DISARANKAN OLEH  
NATIONAL INSTITUTE OF  
STANDARDS AND  
TECHNOLOGY (NIST)  
ADA BEBERAPA ASPEK  
YANG DISARANKAN OLEH  
NIST UNTUK MEMPERKUAT  
PASSWORD KITA

# STANDAR PASSWORD

---

## REKOMENDASI UNTUK PENGGUNA



Menggunakan Password Manager



Menggunakan Multifactor Authentication (MFA)

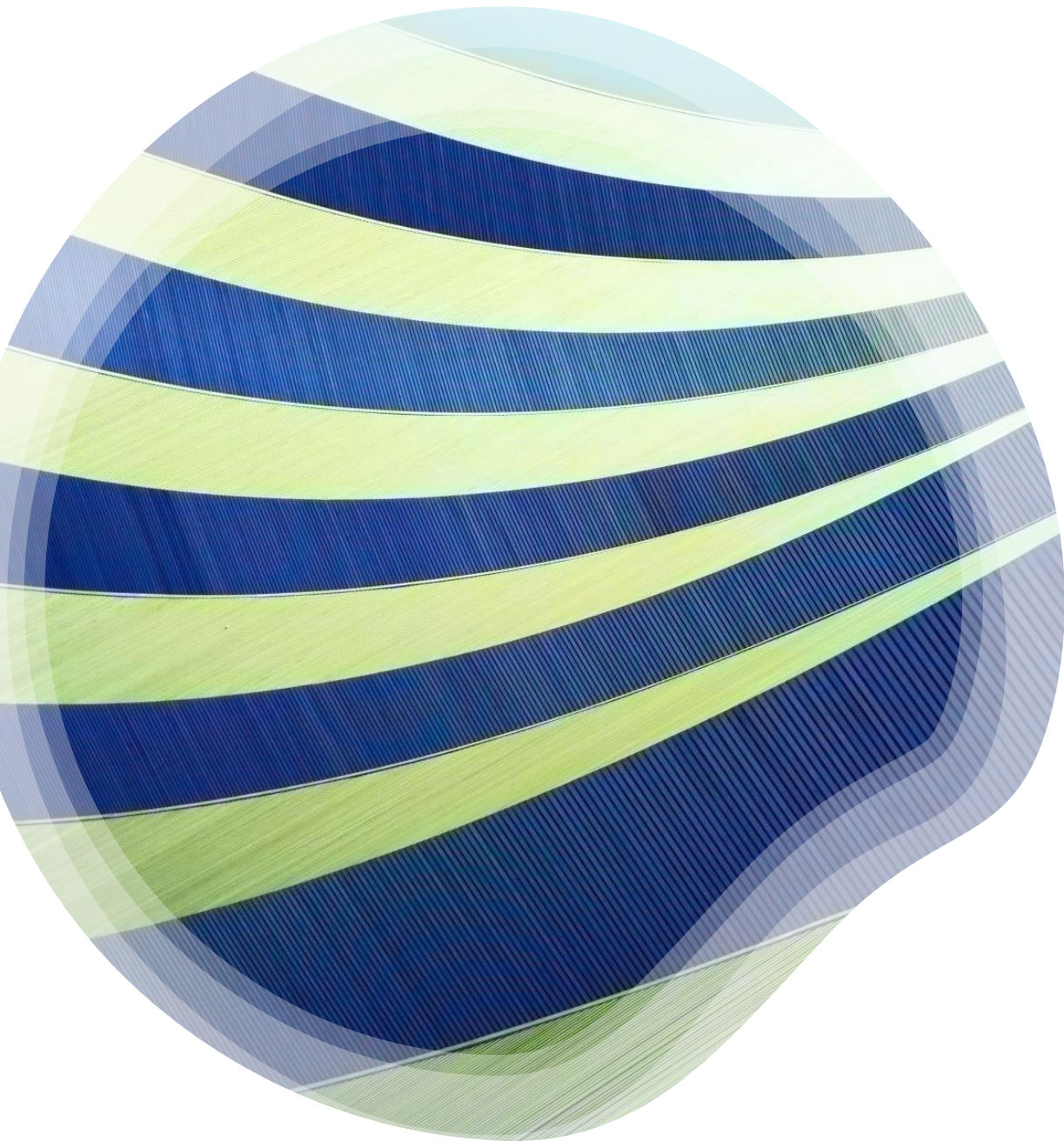


Disarankan membangun password yang panjang – bukan hanya kompleks



Segera mengganti password apabila password sudah bocor





## Membangun Password (yang sulit dibobol dan mudah diingat!)



Hashing memberi kita keuntungan untuk bisa membuat password dengan pola tertentu tanpa diketahui oleh pihak tidak bertanggungjawab



Cukup dengan mengingat 2-3 password “utama”, kita bisa membangun puluhan hingga ratusan password yang bisa digunakan untuk semua akun kita!



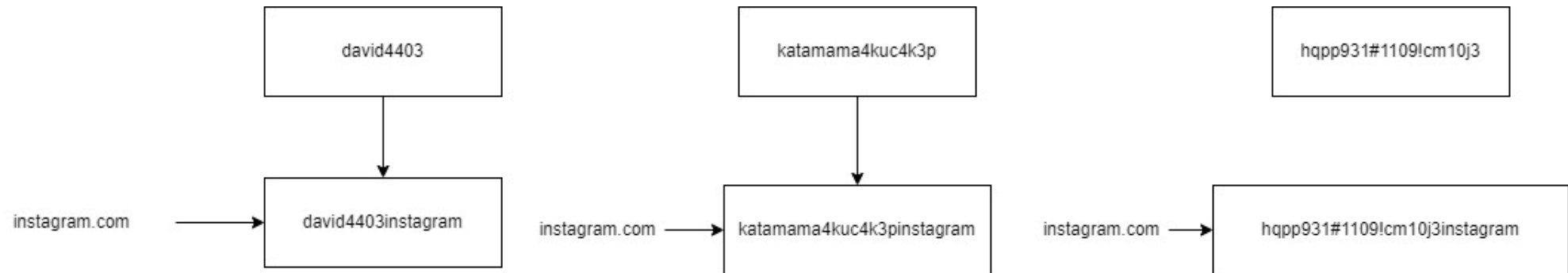
Gimana caranya ya?

# Master Password

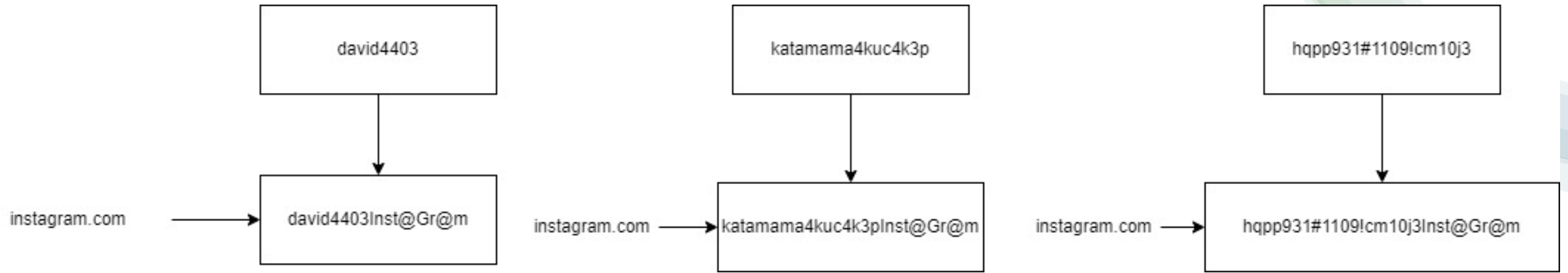
- Buat 3 Master Password.  
Usahakan master password ini memiliki fungsi yang berbeda, dan memiliki kompleksitas berbeda dari biasa, penting, hingga sangat penting

# Contoh

david4403	katamama4kuc4k3p	hqpp931#1109!cm10j3
-----------	------------------	---------------------

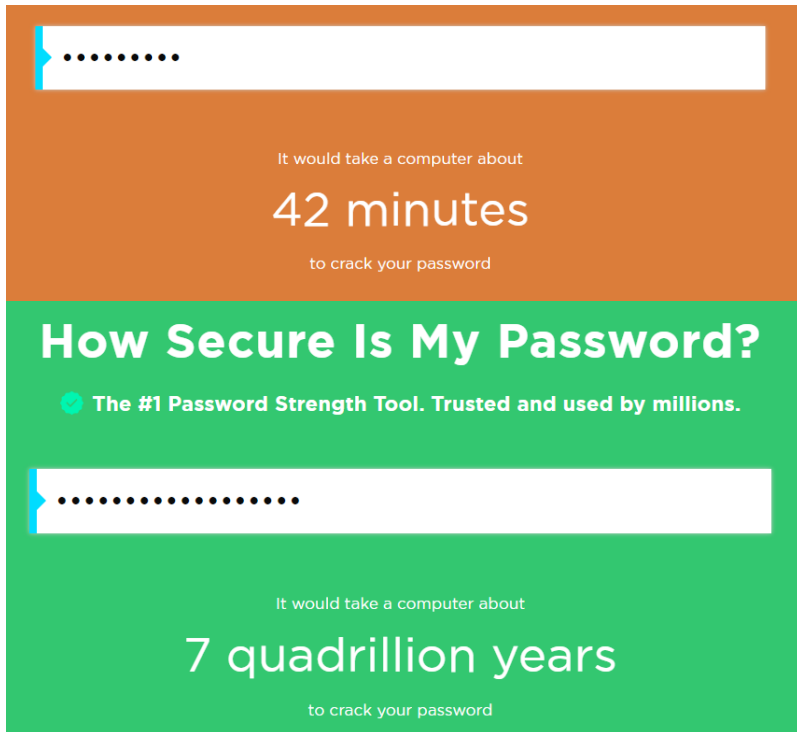


Kombinasikan master password tersebut dengan nama website yang akan diregister



VARIASIKAN GABUNGAN PASSWORD!

# CEK KEKUATAN PASSWORD...



.....

It would take a computer about  
**42 minutes**  
to crack your password

### How Secure Is My Password?

🟢 The #1 Password Strength Tool. Trusted and used by millions.

.....

It would take a computer about  
**7 quadrillion years**  
to crack your password



.....|

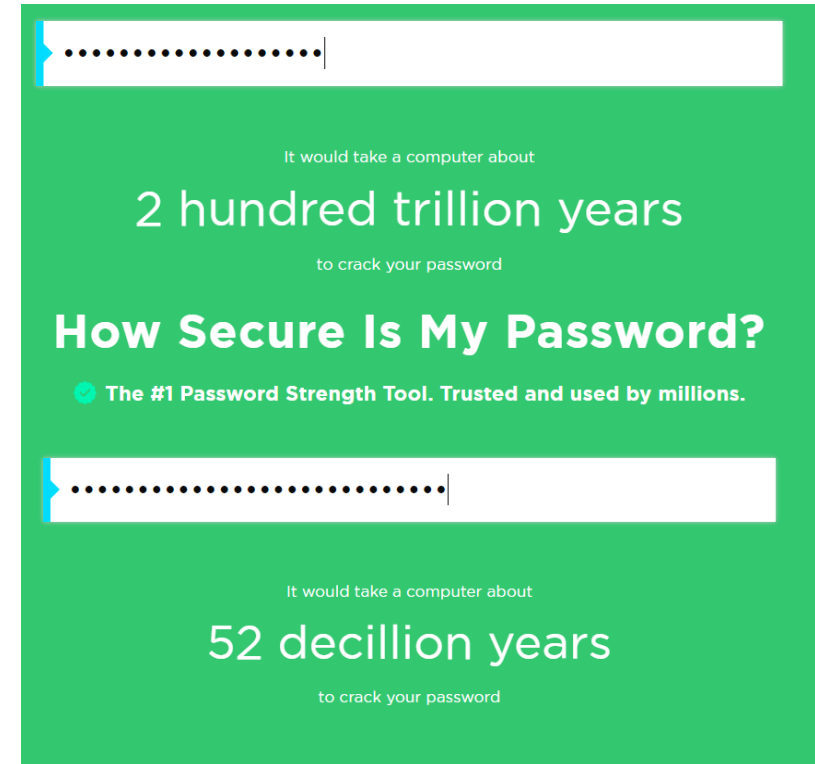
It would take a computer about  
**6 million years**  
to crack your password

### How Secure Is My Password?

🟢 The #1 Password Strength Tool. Trusted and used by millions.

.....|

It would take a computer about  
**1 hundred octillion years**  
to crack your password



.....|

It would take a computer about  
**2 hundred trillion years**  
to crack your password

### How Secure Is My Password?

🟢 The #1 Password Strength Tool. Trusted and used by millions.

.....|

It would take a computer about  
**52 decillion years**  
to crack your password

Quadrillion : 1,000,000,000,000,000  
Octillion : 1,000,000,000,000,000,000,000,000,000  
Decillion : 1,000,000,000,000,000,000,000,000,000,000,000

## Encrypt

Encrypt some text. The result shown will be a Bcrypt encrypted hash.

```
$2a$12$iFVIXgZvY2mMIHXTdg0px.HC.6rse93vfMGYyr.k95r6wfz5q45Pm
```

Encrypt

## Encrypt

Encrypt some text. The result shown will be a Bcrypt encrypted hash.

```
$2a$12$8M0ja7gPazGwtDTzvK7DK.1aahrcAaqeJzmSEVHoCYkZzwpqqb4rq
```

Encrypt

```
$2a$12$2dOJAWWVofiu4Pc/46eFC.Itec3nQLE0AQJ4AKJmdTyC20SY0iQcW
```

Encrypt

+

o

# CEK HASH PASSWORD...

# Keuntungan dan kerugian

- (+) Password lebih kuat namun masih bisa diingat
- (+) Setiap akun akan memiliki password yang unik. Jika ada data bocor di salah satu website, yang terkena impact hanya akun di website tersebut.
- (+) Tidak perlu pikir panjang ketika mau membuat akun “bodong” di situs yang tidak terlalu penting (seperti email marketing untuk dapat produk gratis)
- (-) Sesekali diperlukan penggantian master password dan perlu mengubah seluruh password. Atau bahkan malah menambah master password.
- (-) Jika ada sisihan uang bulanan, ada baiknya untuk membeli password manager karena lebih mudah manage semua password di satu platform

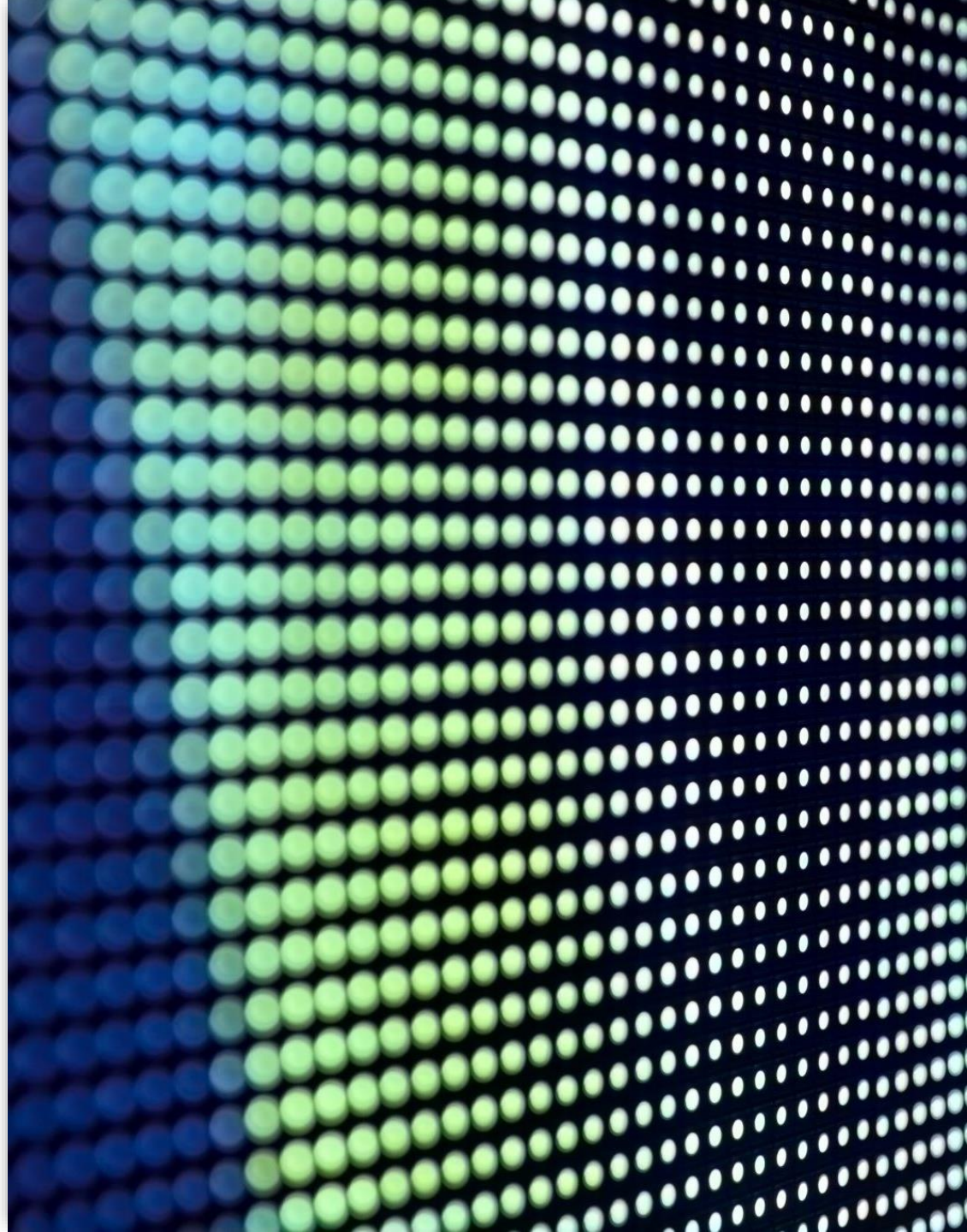




# Multi Factor Authentication

# Multifactor Authentication

- Kalau teman-teman pernah masuk ke website, kemudian website tersebut meminta kode yang dikirimkan ke SMS untuk bisa masuk?
- Itu salah satu contoh Multifactor Authentication!
- SMS itu ada OTP atau One-time Password



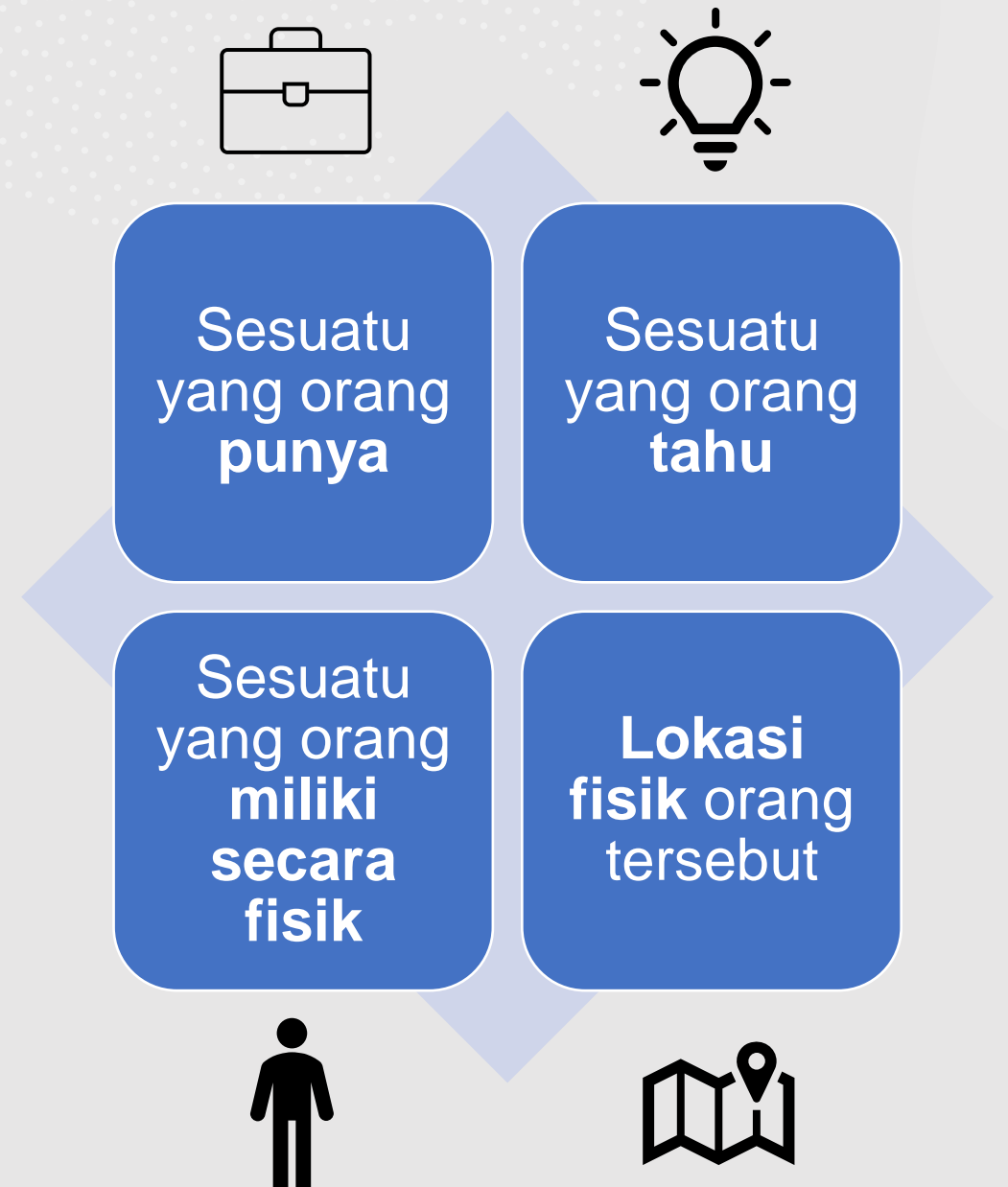


# Apa itu Multifactor Authentication

Multifactor authentication adalah metode autentikasi yang digunakan untuk mengakses sebuah website atau layanan dengan menunjukkan **lebih dari satu** “faktor” kepada system tersebut.

MFA adalah sistem berlapis yang diterapkan untuk menjaga data pribadi supaya ketika terjadi keteledoran atau kebocoran, masih perlu ada satu kali autentikasi lagi.

# The “Factor”



# CONTOH MASING-MASING FAKTOR

---

- Sesuatu yang orang **punya**

- USB Stick
- Kartu ATM
- Kartu ID Card



- Sesuatu yang orang **tahu**

- Password
- PIN
- Pertanyaan keamanan



- Sesuatu yang orang **miliki secara fisik**

- Sidik jari
- Iris mata
- Wajah



- **Lokasi fisik** orang tersebut

- GPS
- IP Address

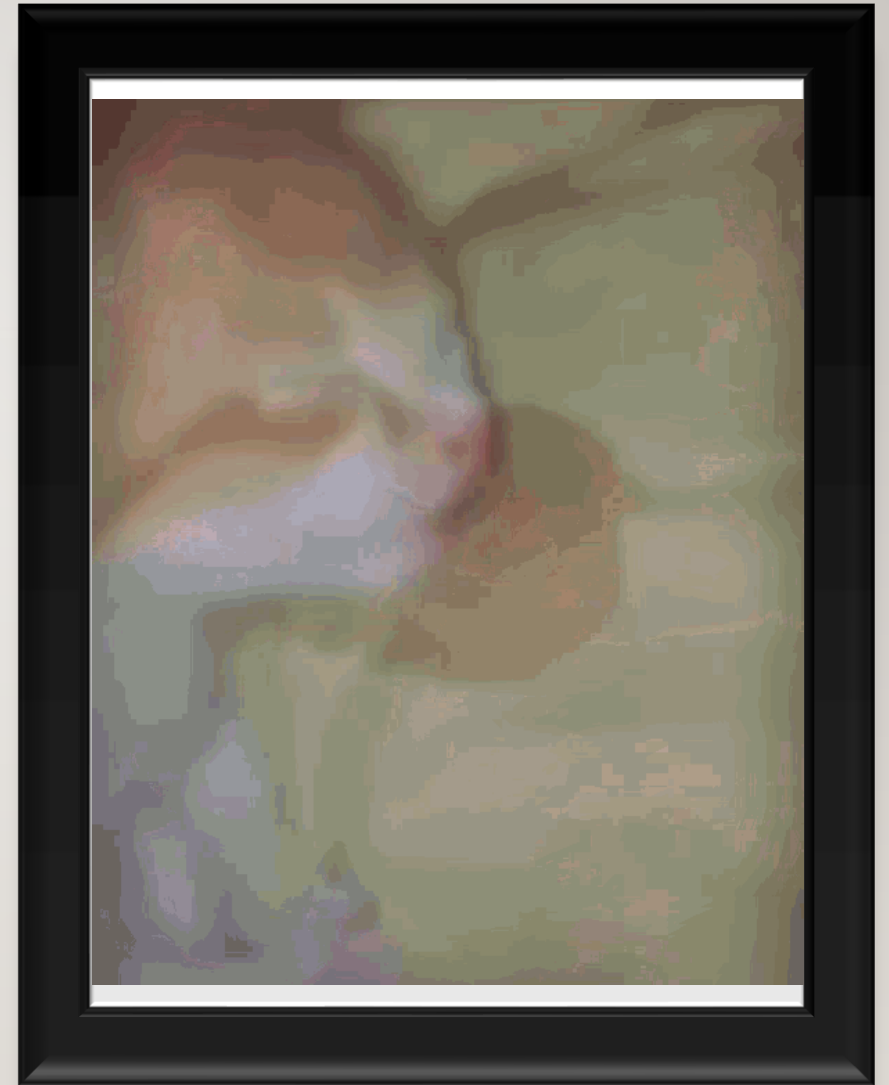


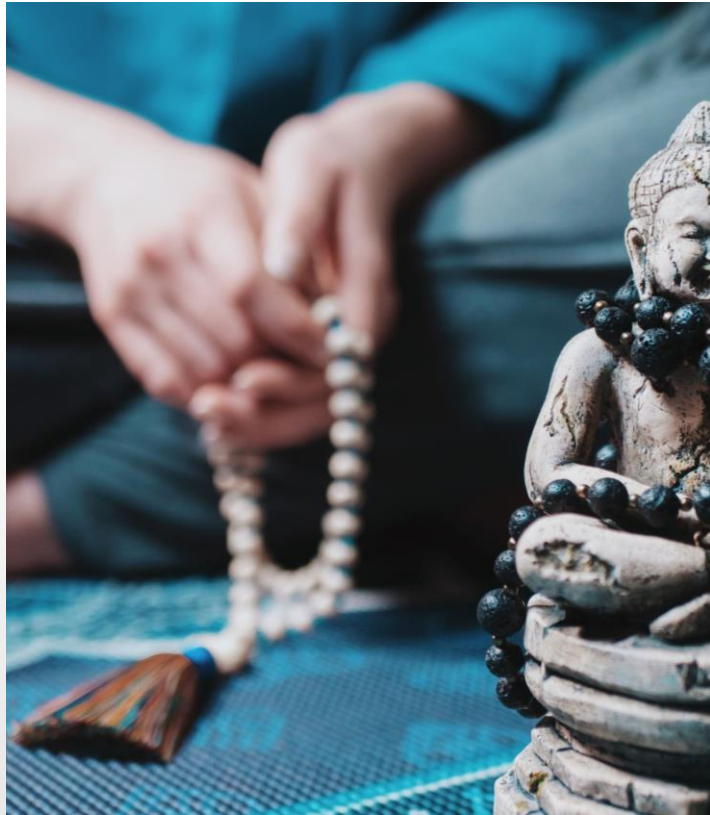
# MEREPOTKAN?

---

Tentu saja! Tapi jika dibandingkan dengan asset teman-teman yang mungkin sangat berharga, kerepotan kecil ini sangat-sangat membantu.

Terlebih lagi ini merupakan standar emas yang saat ini digunakan di perusahaan besar untuk mengamankan asset tertentu.





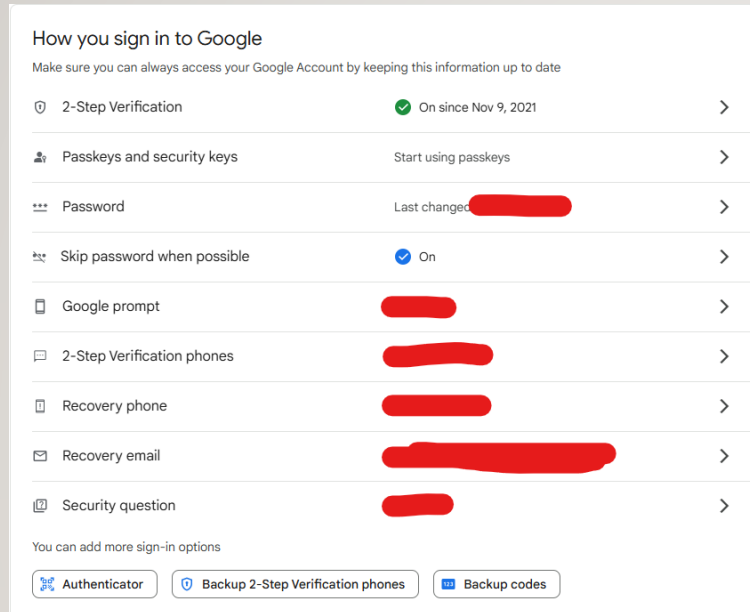
# BAGAIMANA CARA MEMULAINYA?

---

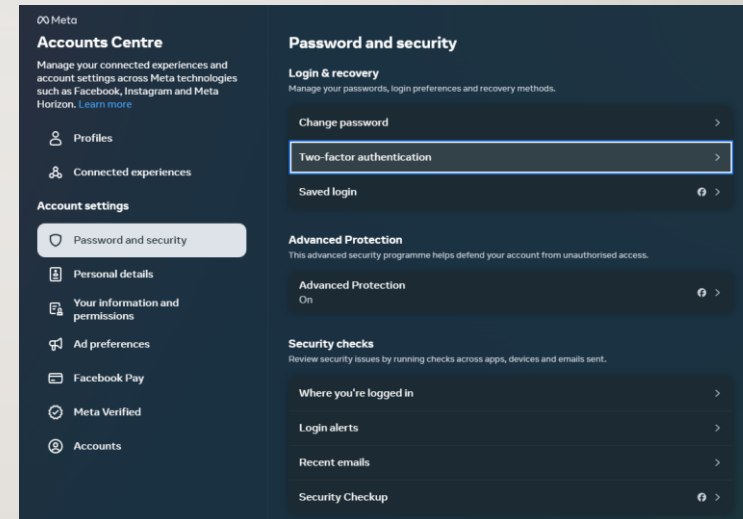
TIDAK SEMUA LAYANAN MEMILIKI OPSI UNTUK MEMBERIKAN MFA PADA AKUN TEMAN-TEMAN.

TAPI PADA AKUN-AKUN DI LAYANAN BESAR SEPERTI GOOGLE, FACEBOOK, INSTAGRAM, SEMUANYA PUNYA CARA UNTUK MENYALAKAN MFA

## Google (myaccount.google.com/security)



## Facebook (https://accountscenter.facebook.com/password\_and\_security/two\_factor)



---

# CONTOH LOKASI SETTING MFA



Is SMS 2FA secure?

No.

**FIX AMAN DONG?**

---

BELUM TENTU... WALAUPUN BEGITU, ADA BEBERAPA FACTOR YANG MASIH BERISIKO SEPERTI SMS.

## **An Empirical Study of Wireless Carrier Authentication for SIM Swaps**

Presented at [SOUPS 2020](#)

Akses untuk melihat dan mengirim SMS. Dengan izin akses ini, aplik  
baca isi SMS yang ada pada *smarthphone* korban. Hal ini sangat berbahaya  
t dimanfaatkan untuk **penyadapan SMS** termasuk **kode OTP** atau verifikasi

```
<uses-permission  
  name='android.permission.RECEIVE_SMS'>  
</uses-permission>  
<uses-permission  
  name='android.permission.INTERNET'>  
</uses-permission>  
<uses-permission  
  name='android.permission.READ_SMS'>  
</uses-permission>  
<uses-permission  
  name='android.permission.SEND_SMS'>  
</uses-permission>
```

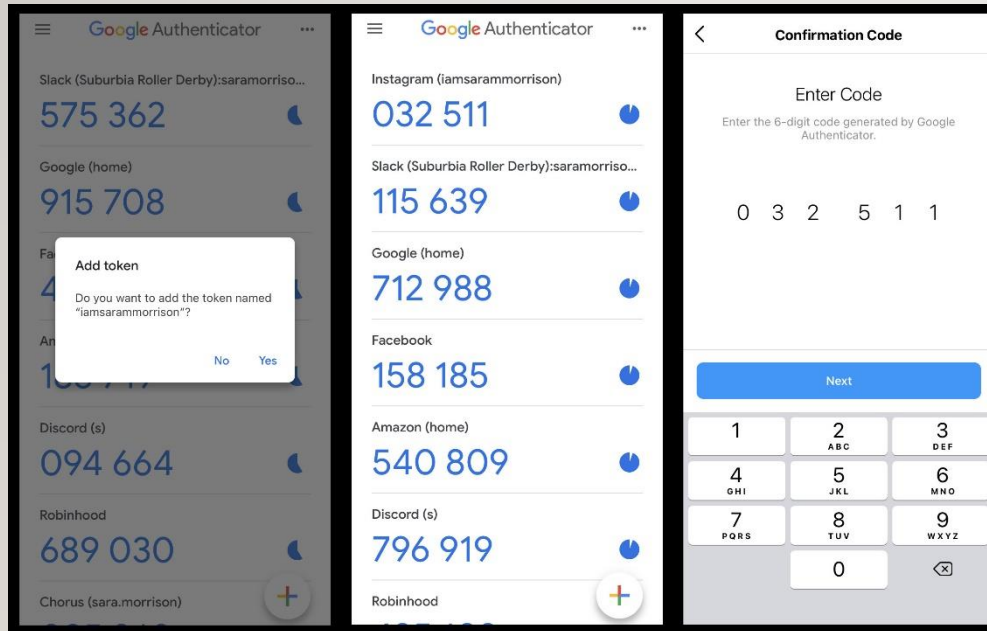
Gambar 5 Application Permission file APK



## SMS MFA TIDAK AMAN?

- Kalau teman-teman ingat, kita sempat heboh dengan adanya undangan pernikahan yang berbentuk APK.
- Aplikasi ini sebenarnya ada **Virus** dan aplikasi ini **bisa membaca SMS**. Sehingga jika teman-teman punya MFA berupa SMS, jika pernah memasang ini, pelaku juga tau kode rahasianya yang bisa membuat pelaku membobol akun teman-teman.

# AUTHENTICATOR



- Authenticator adalah aplikasi untuk menyediakan OTP
- Tanpa perlu sinyal, bahkan ketika HP mode pesawat, OTP masih bisa didapatkan
- Lebih aman dari serangan “APK”



Google Authenticator



Microsoft Authenticator

# MEMULAINYA

---

# LANGKAH MEMULAI (SECARA UMUM)

---

- Memasang app authenticator
- Buka akun yang akan dipasang authenticator
- Cari bagian “keamanan” atau “security”
- Cari bagian “2 Factor Authentication” atau “Multi Factor Authentication”, kemudian tambahkan
- Akan diminta untuk scan QR Code, caranya dengan membuka app authenticator, kemudian cari icon “+” dan pilih “scan QR Code”

# FACEBOOK, INSTAGRAM, THREADS

HTTPS://ACCOUNTSCENTER.F  
ACEBOOK.COM/PASSWORD\_A  
ND\_SECURITY/TWO\_FACTOR

## Two-factor authentication is on

We'll now ask for a login code whenever you log in on a device that we don't recognise. [Learn more](#)

### How you get login codes

**Authentication app**  
**Recommended** • You'll get a login code from your authentication app. >

**Additional methods**  
See how to log in securely even if your other methods aren't available. >

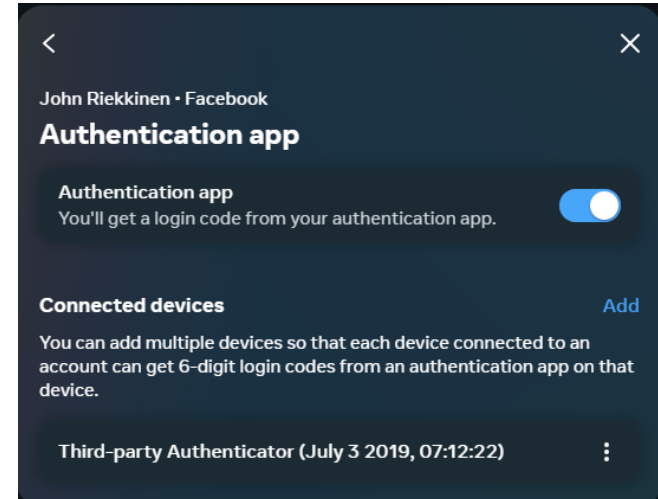
### Add a backup method

**Text message**  
We'll send a code to the number that you choose. >

**Security keys**  
Use physical security keys to protect your account from unauthorised access. You must have this key with you to log in from an unrecognised device. >

### Authorised logins

**Trusted devices**  
Review a list of devices on which you won't have to use a >



# GOOGLE

HTTPS://MYACCOUNT.GOOGLE.COM/SIGNI  
NOPTIONS/TWOSV

## ← Verifikasi 2 Langkah

### Akun Anda dilindungi dengan Verifikasi 2 Langkah

Cegah peretas mengakses akun Anda dengan lapisan keamanan tambahan.







Kecuali jika Anda login dengan kunci sandi, Anda akan diminta untuk menyelesaikan langkah kedua paling aman yang tersedia di akun Anda. Anda dapat memperbarui langkah kedua dan opsi login Anda kapan saja di setelan Anda. [Buka Setelan Keamanan](#) ⇄



[Nonaktifkan Verifikasi 2 Langkah](#)

### Langkah kedua

Pastikan Anda dapat mengakses Akun Google Anda dengan terus memperbarui informasi ini dan menambahkan lebih banyak opsi login

- |  |  |   |
|--|--|---|
|  Kunci sandi dan kunci keamanan |  Tambahkan kunci keamanan             | > |
|  Dialog Google                  |  1 perangkat                          | > |
|  Authenticator                |  Tambahkan aplikasi pengautentikasi | > |

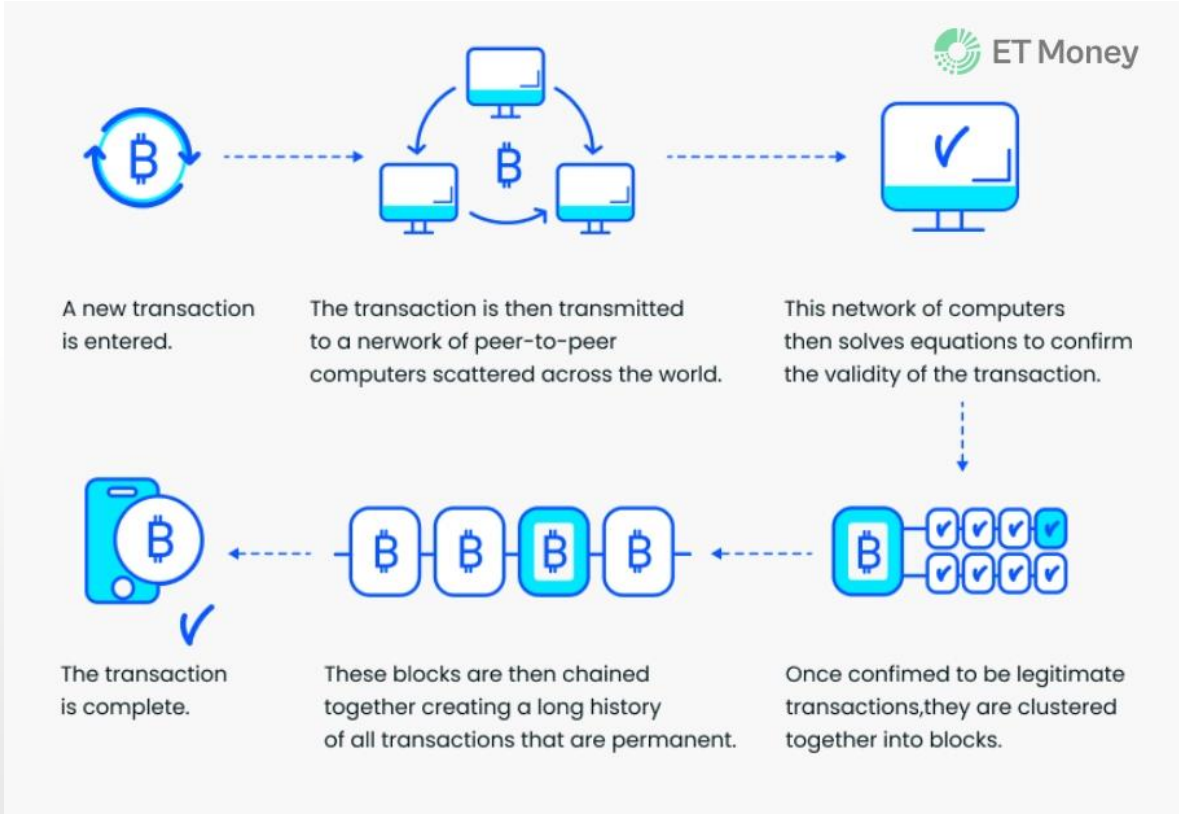


Cryptocurrency



# CRYPTO CRYPTO LEBIH DARI UANG

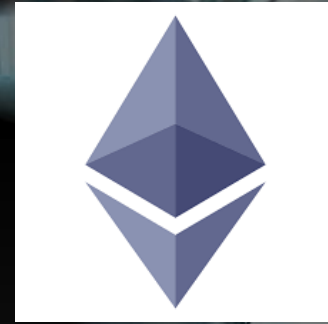
- Cryptocurrency atau biasa kita kenal sebagai Crypto adalah sebuah mata uang digital yang didesain sedemikian rupa agar tidak memiliki pihak yang “berwenang” atau decentralized.
- Awal diciptakan oleh Satoshi Nakamura untuk anonimitas, supaya transaksi bisa berjalan secara mandiri tanpa ada pengawasan pihak manapun



# CARA KERJA CRYPTO

# CONTOH CRYPTO

- Bitcoin
- Ethereum
- Binance Coin
- Dogecoin



## REALITANYA?

- Karena sifatnya yang anonim, cryptocurrency seringkali digunakan untuk transaksi ilegal, dari narkoba, senjata, pembayaran ransom, hingga pemerasan digital (extortion)
- Tidak ada wewenang yang mengatur membuat transaksi tidak bisa dijelaskan asal dan tujuannya
- Karena siapapun bisa membuat mata uang baru, crypto sering digunakan untuk tempat penipuan mata uang. “Rugpull”
- Ingat, cryptocurrency adalah **mata uang**

# CARA MENYIKAPI CRYPTO SUPAYA TIDAK TERKECOH

- Crypto adalah **mata uang**. Jika ada seseorang yang mengklaim crypto adalah investasi agar cepat **kaya**, kemungkinan besar itu adalah **penipuan**.
- Walaupun transaksi crypto anonim, karena desainnya transaksi harus dibuat public, bahkan biro investigasi seperti FBI juga bisa memonitor transaksinya.
- Secara fungsi, cryptocurrency hampir tidak ada bedanya dengan uang digital seperti Gopay, OVO, atau bahkan mobile banking – bedanya hanya crypto tidak diawasi badan seperti OJK, BI, atau Federal Reserve System



# Generative AI

# GENERATIVE AI

---

Artificial Intelligence (AI) atau Kecerdasan Buatan adalah “kemampuan sistem untuk menafsirkan data eksternal dengan benar, untuk belajar dari data tersebut, dan menggunakan pembelajaran tersebut guna mencapai tujuan dan tugas tertentu melalui adaptasi yang fleksibel”

Generative AI atau Kecerdasan Buatan Generatif adalah jenis kecerdasan buatan yang mampu membuat teks, gambar, video, audio, dan data lainnya dari model generatif, yang umumnya berdasarkan input prompt.



---

# THÉÂTRE D'OPÉRA SPATIAL

MIDJOURNEY



# KEGUNAAN GENERATIVE AI

---

Bisa membuat hampir media apapun berdasarkan masukan yang kita berikan (prompt).

Dapat disesuaikan apabila hasil tidak sesuai dengan keinginan

Tidak perlu atribusi

Relatif terjangkau

---

## KEKURANGAN GENERATIVE AI

Lisensi belum jelas, karena konten hasil scraping

Penggunaan masih di sisi riset dan “for fun”

Kontroversial untuk penggunaan komersil, sulit untuk digunakan ke bisnis digital

Hasil seringkali janggal dan tidak “manusia”

The background features a complex network of thin, light blue lines connecting various-sized blue circles. The circles range from small dots to larger, semi-transparent spheres. The overall effect is a dynamic, interconnected pattern that resembles a molecular structure or a data network. The circles are more densely packed in the upper right and lower right areas, with some overlapping to create darker shades of blue.

THANK YOU!

---