



UNIVERSITI  
TEKNOLOGI  
MARA

# eLatihan: Taklimat Keselamatan ICT

---

Ts. Mohd Firdaus Fairoz bin Zairolazhar

30 Jun 2021

Anjuran: Perpustakaan Tun Abdul Razak (PTAR), UiTM

# TAKLIMAT KESELAMATAN ICT

- Taklimat ini memberi pendedahan mengenai keselamatan ICT sebagai pengguna.
- Di akhir taklimat ini, anda boleh:
  - Mengetahui prinsip keselamatan ICT
  - Mengetahui ancaman dan risiko keselamatan ICT
  - Mengetahui kaedah menjaga keselamatan ICT

# KANDUNGAN

1

Pengenalan

Akses Keselamatan

2

3

Keselamatan Maklumat

Keselamatan Emel

4

5

Penyelenggaraan Keselamatan ICT

Aduan Keselamatan ICT

6

# Global Digital Report – Jan 2021

Populasi Malaysia  
32.57 juta orang

Pengguna Internet

84% daripada populasi

Pengguna Aktif Social Media

86% daripada populasi

Langganan Mobile

39.99 juta akaun

Sumber: <https://datareportal.com/>

## Global Digital Report – Jan 2021 (samb.)

Purata masa penggunaan  
Internet sehari



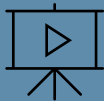
9 Jam 17 Minit

Purata masa penggunaan  
Social Media sehari



3 Jam 01 Minit

Purata masa menonton TV  
/ Streaming Media sehari



2 Jam 55 Minit

Purata masa mendengar  
muzik (streaming) sehari

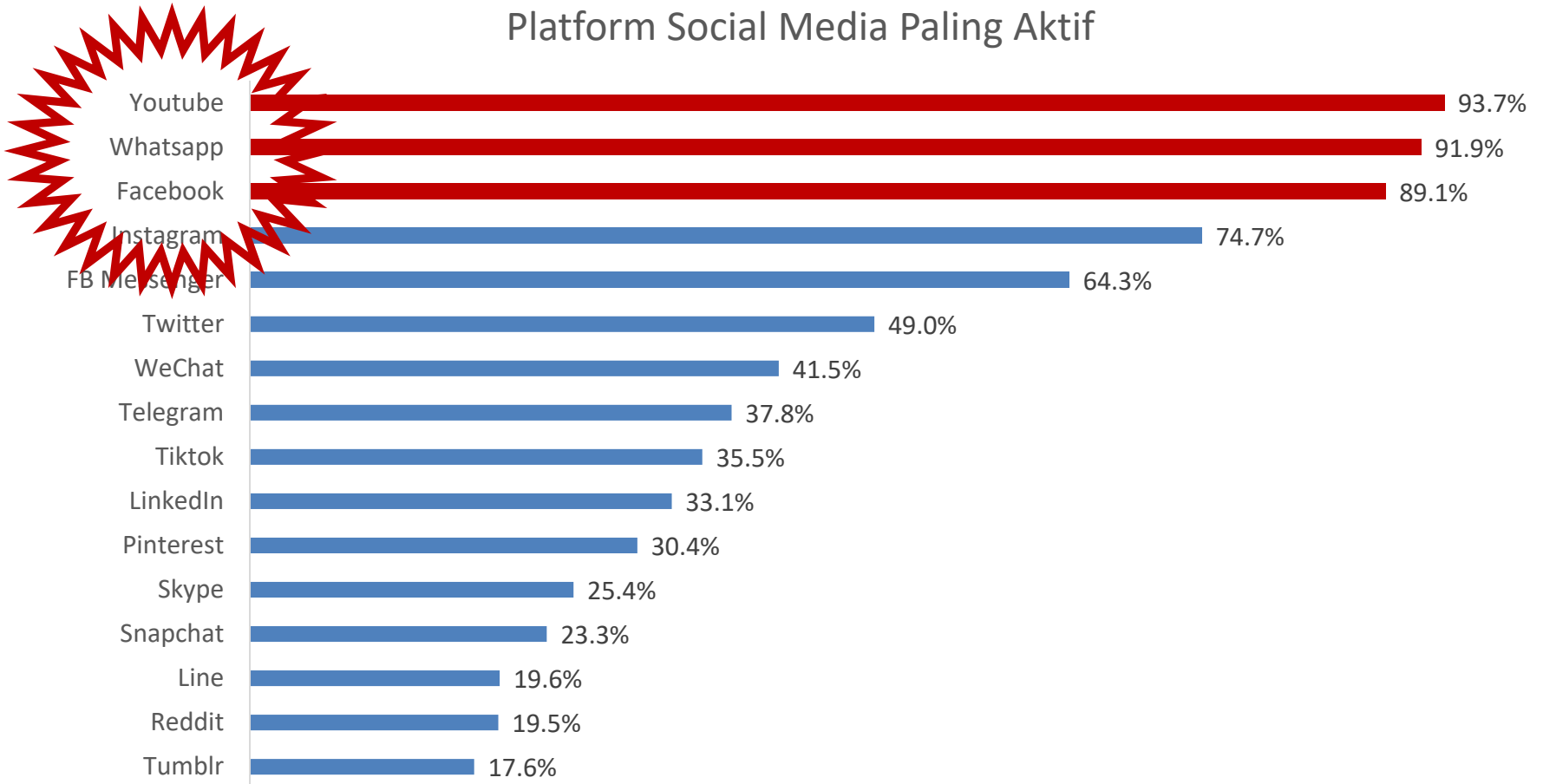


1 Jam 35 Minit

Sumber: <https://datareportal.com/>

# Global Digital Report – Jan 2020 (samb.)

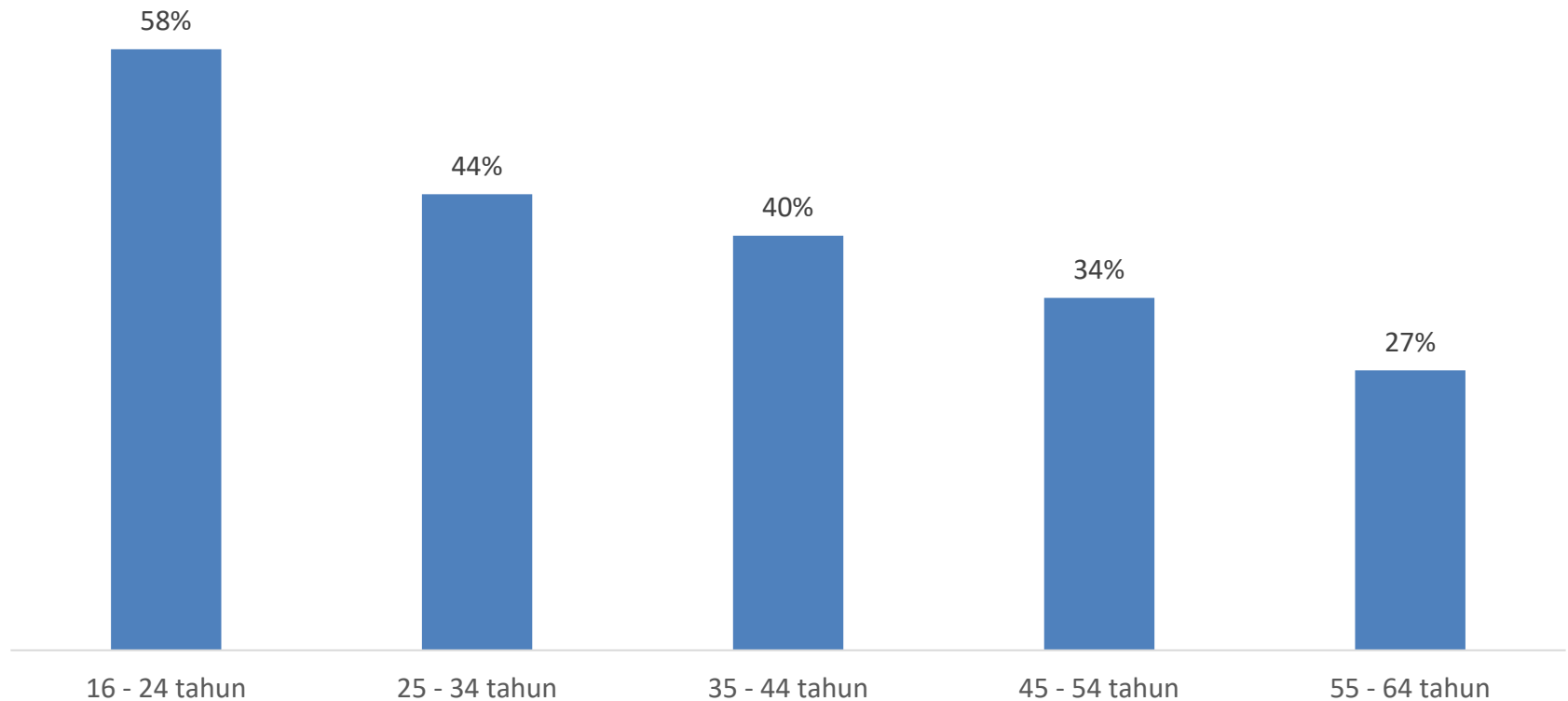
## Platform Social Media Paling Aktif



Sumber: <https://datareportal.com/>

# Global Digital Report – Julai 2020

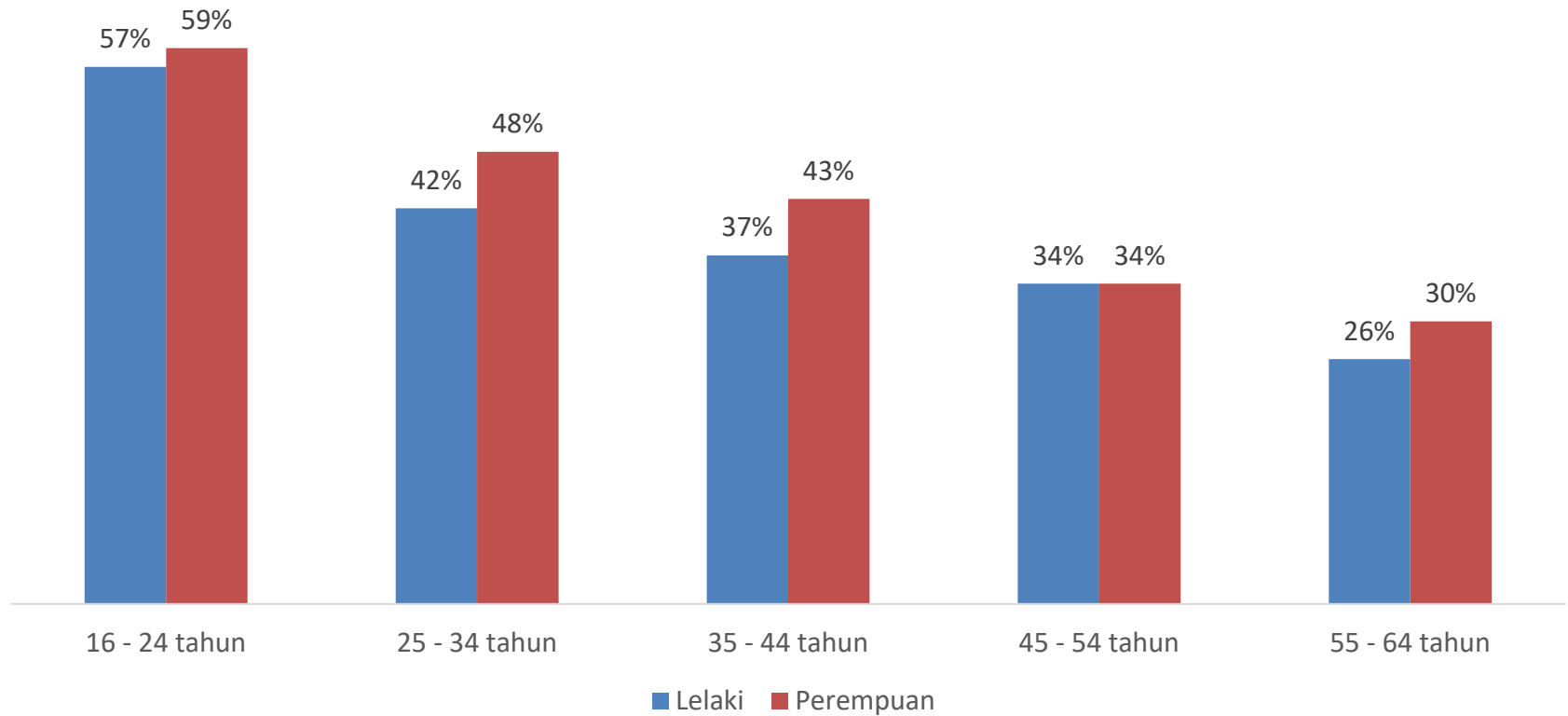
Covid-19: Peningkatan Penggunaan Media Sosial Berdasarkan Kumpulan Umur



Sumber: <https://datareportal.com/>

# Global Digital Report – Julai 2020 (samb.)

Covid-19: Peningkatan Penggunaan Media Sosial Berdasarkan Kumpulan Umur



Sumber: <https://datareportal.com/>





# Global Cybersecurity Index 2018

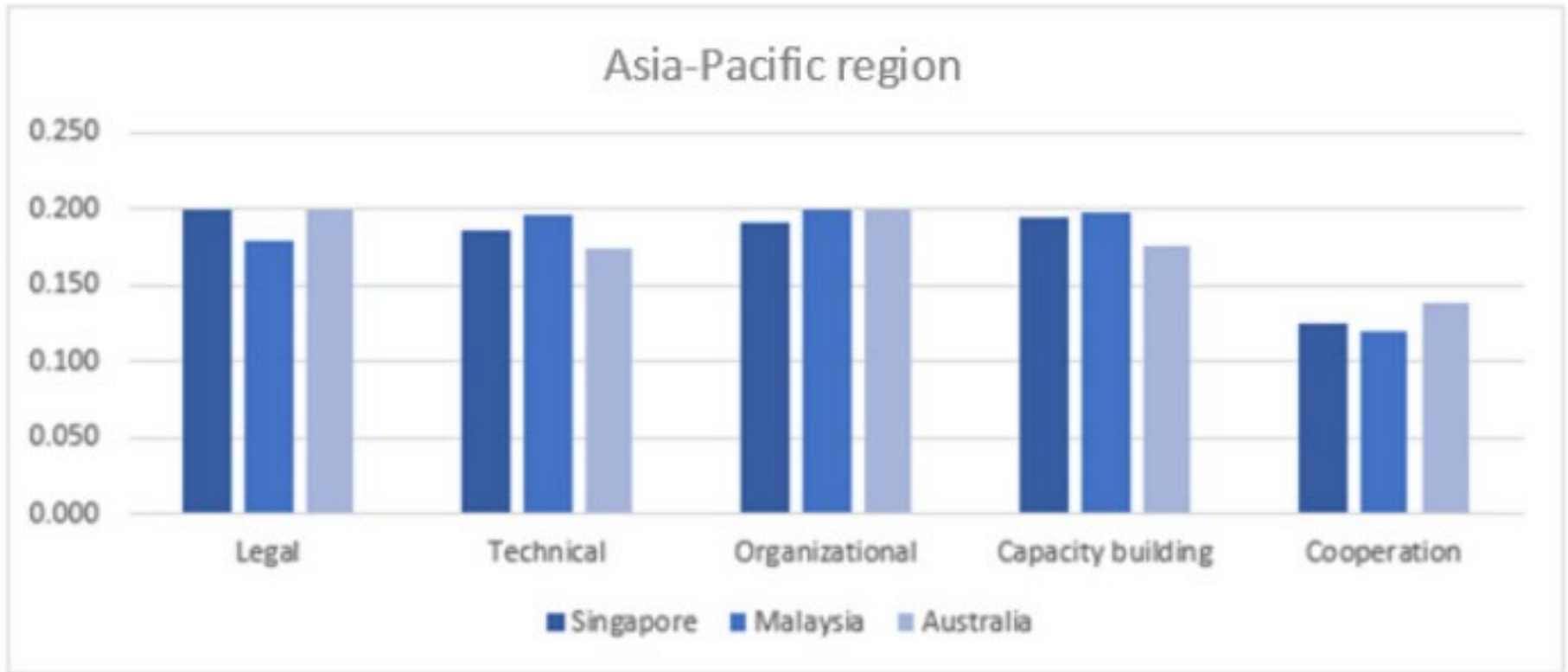
## Annex B: Global ranking GCI 2018

*The countries marked with an \* are countries that did not participate in GCI 2018. They have neither submitted their answers to the questionnaire nor validated the data collected by the GCI team.*

Member State	Score	Global Rank
United Kingdom	0.931	1
United States of America*	0.926	2
France	0.918	3
Lithuania	0.908	4
Estonia	0.905	5
Singapore	0.898	6
Spain	0.896	7
Malaysia	0.893	8
Canada*	0.892	9
Norway	0.892	9
Australia	0.890	10

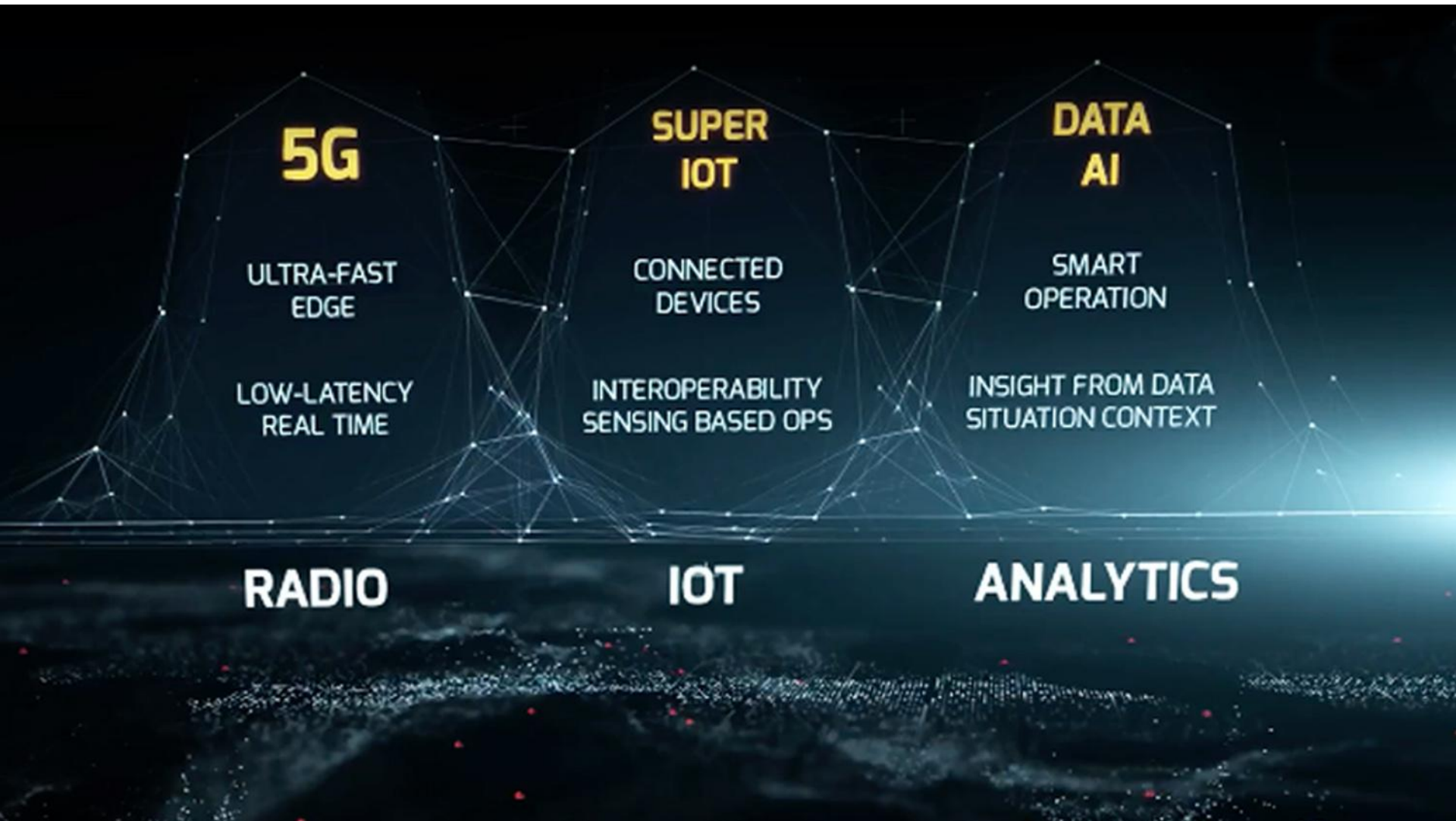
Sumber: ITU Telecommunication Development

# Global Cybersecurity Index 2018 (samb.)

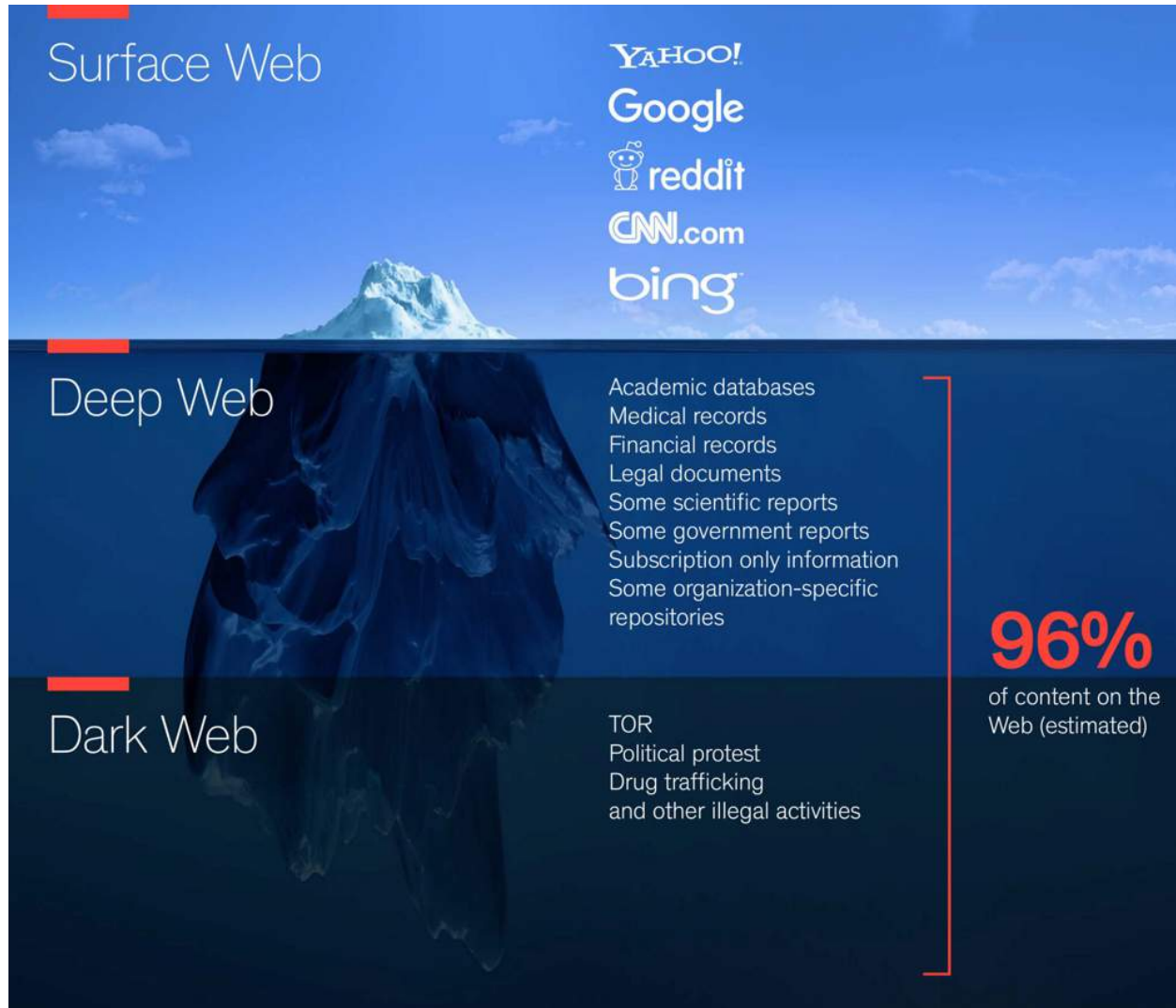


Sumber: ITU Telecommunication Development

# Intelligent Connectivity – 2021



# Gambaran Web



# Ancaman Siber

				
Penipuan Atas Talian			Serangan ke atas infrastruktur maklumat kritikal negara	Kandungan Internet (negatif), laman web & blog yang mempengaruhi fikiran masyarakat

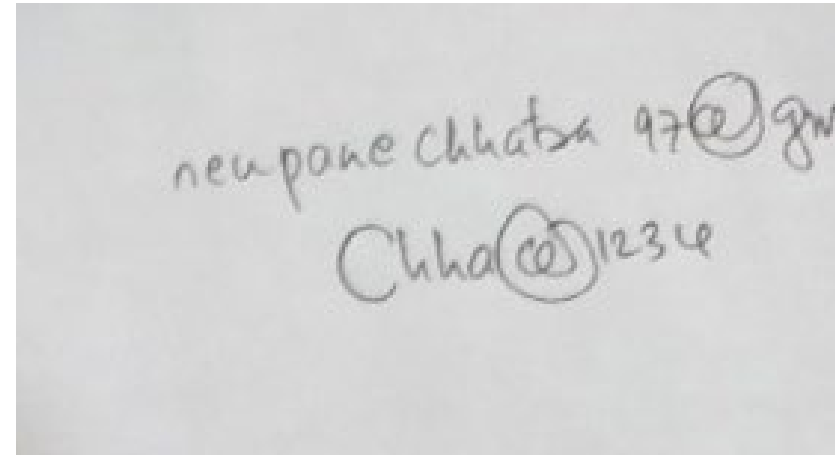
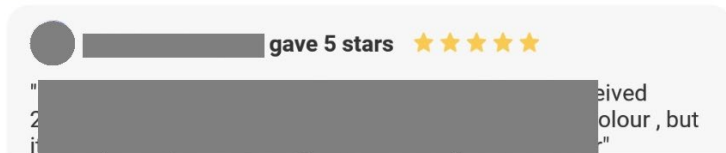
**91% Serangan siber bermula daripada emel**





Store 27.2k Followers

Follow



**Aplikasi apa lagi yang menggunakan akaun email?**

**Media Sosial?**

**Aplikasi pembelian online?**

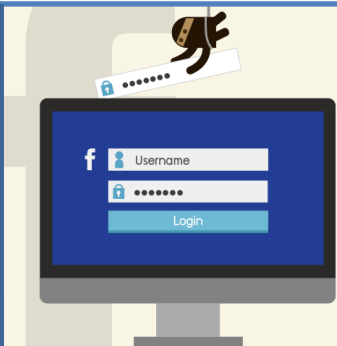
**Maklumat perbankan / kata laluan / peribadi di dalam emel?**

**Adakah kata laluan ini sama untuk aplikasi yang lain?**

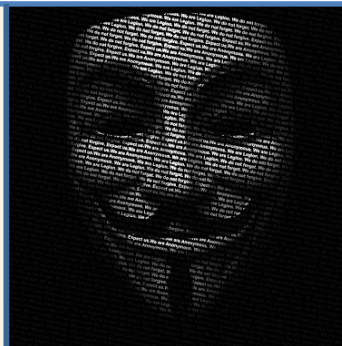
# 5 Jenis Penjenayah Siber



The social engineer



The Spear Phisher



The Hacker



The Rogue Employee



The Ransom Artist

Sumber: Cyber Security Malaysia



# Jenis Penggodam

- **Black Hat**
  - Penggodam yang tidak diberikan kebenaran untuk mengakses sistem komputer dan mengeksploitasi untuk kepentingan peribadi atau kumpulan.
- **White Hat**
  - Penggodam yang diberikan kebenaran oleh pemilik untuk menguji keselamatan sistem komputer dan melaporkan hasil penggodaman kepada pemilik.

## Ancaman Siber (LIVE)



- <https://cybermap.kaspersky.com>



- <https://threatmap.fortiguard.com>



- <https://threatmap.checkpoint.com/ThreatPortal/livemap.html>

Link tersebut adalah betul dan boleh digunakan semasa nota ini disediakan.

# Google Dorking

- “hacked by” site:domain.edu.my
- “greetz” site:domain.edu.my
- “defaced by” site:domain.edu.my

## Google Dorking (samb.)

- “hacked by” site:uitm.edu.my
- “greetz” site:uitm.edu.my
- “defaced by” site:uitm.edu.my
- site:uitm.edu.my filetype:xls
- site:uitm.edu.my filetype:doc

# Isu Semasa Keselamatan ICT

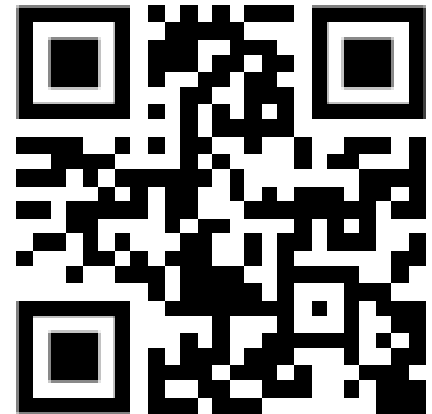
## The Hacker News

Home

Data Breaches

Cyber Attacks

Vulnerabilities



<https://thehackernews.com>

Link tersebut adalah betul dan boleh digunakan semasa nota ini disediakan.



UNIVERSITI  
TEKNOLOGI  
MARA

1

# Pengenalan

# Simulasi Keselamatan

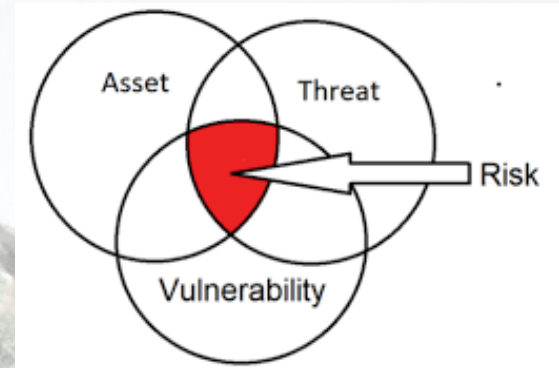
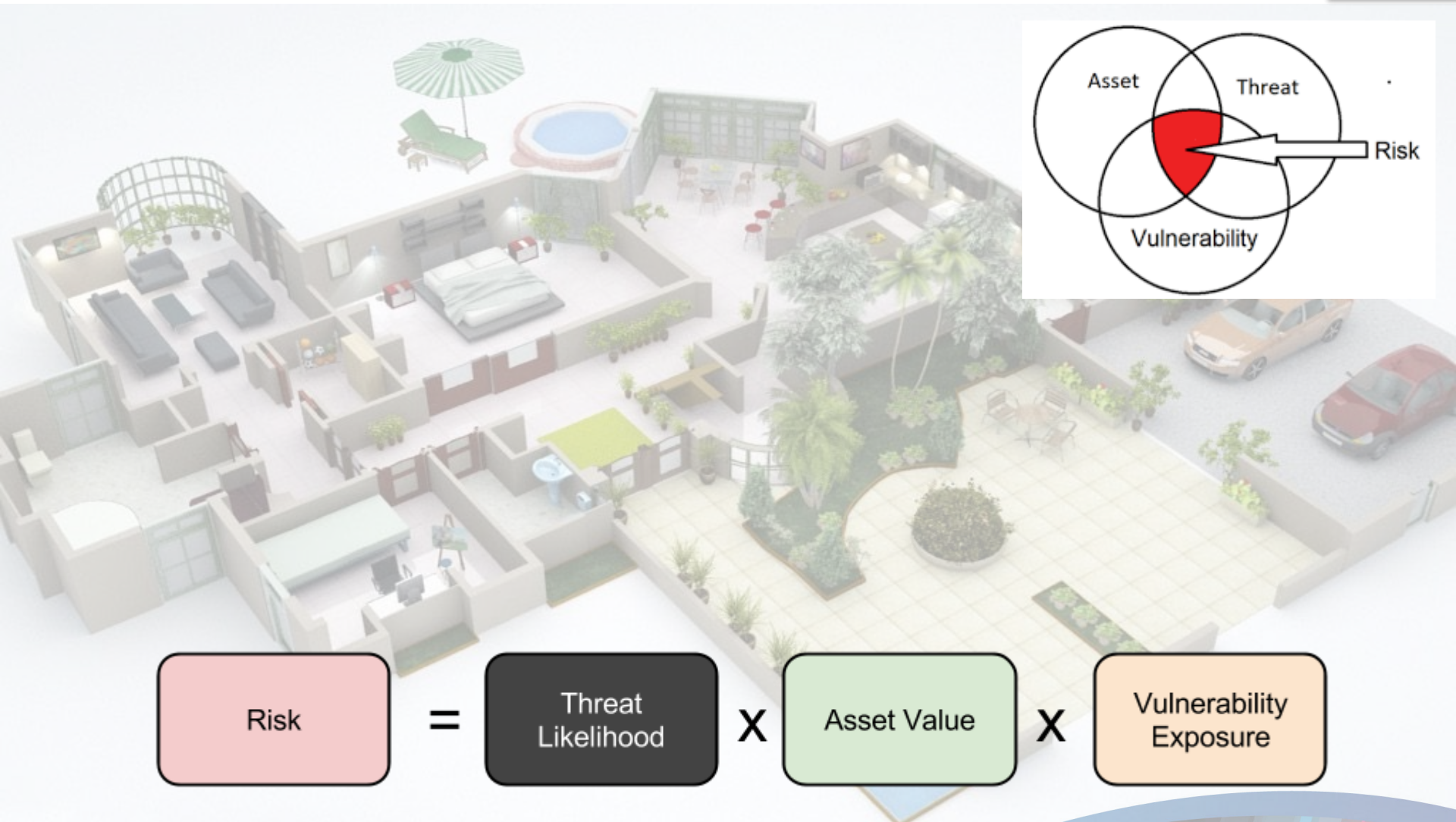
1





# Risiko

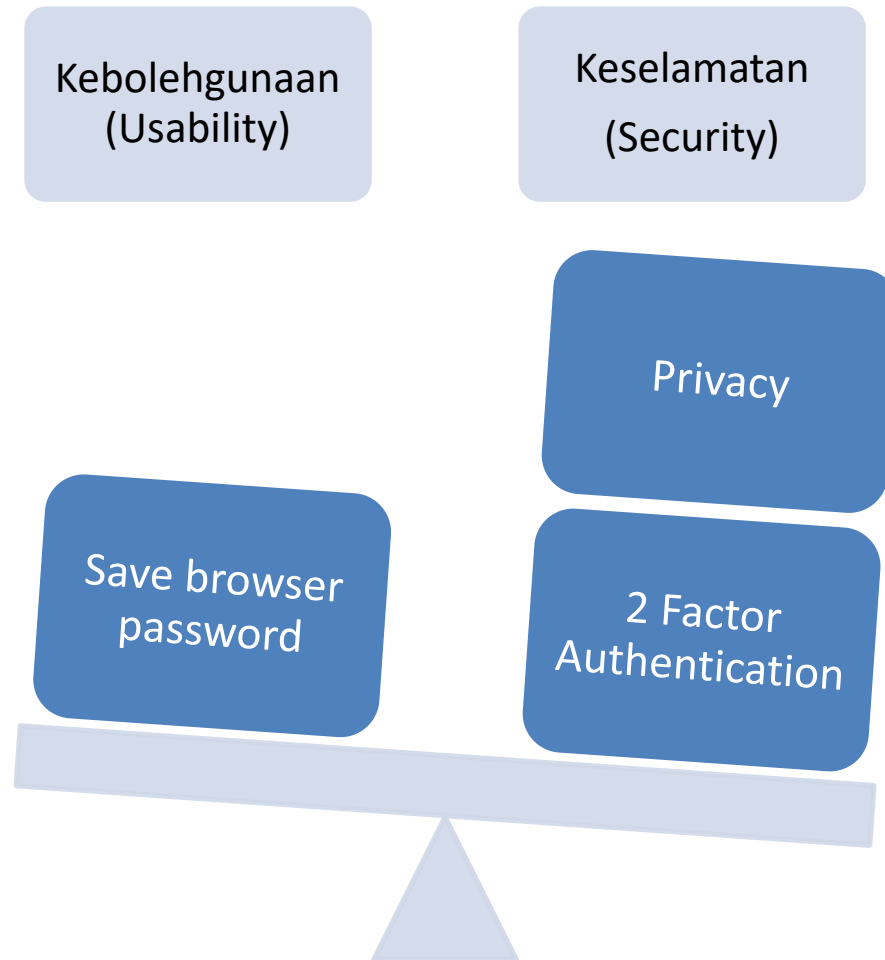
1



$$\text{Risk} = \text{Threat Likelihood} \times \text{Asset Value} \times \text{Vulnerability Exposure}$$



# Keseimbangan Sistem ICT



# Jika mahukan privasi

1

## Lebih privasi

- DuckDuckGo
- iPhone
- Signal
- VPN

## Kurang privasi

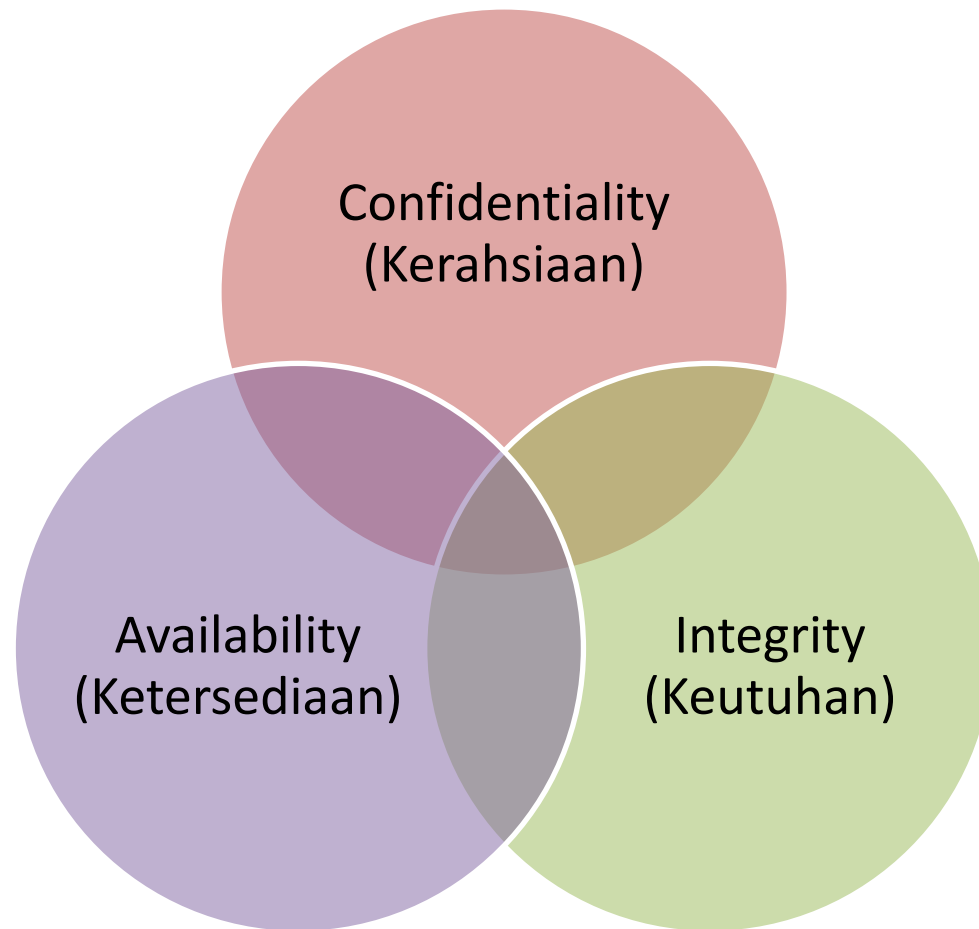
- Google
- Android
- Whatsapp
- Tanpa VPN

Sumber:

<https://www.freemalaysiatoday.com/category/opinion/2021/02/09/5-more-steps-to-stop-your-smartphone-spying-on-you-secretly/>

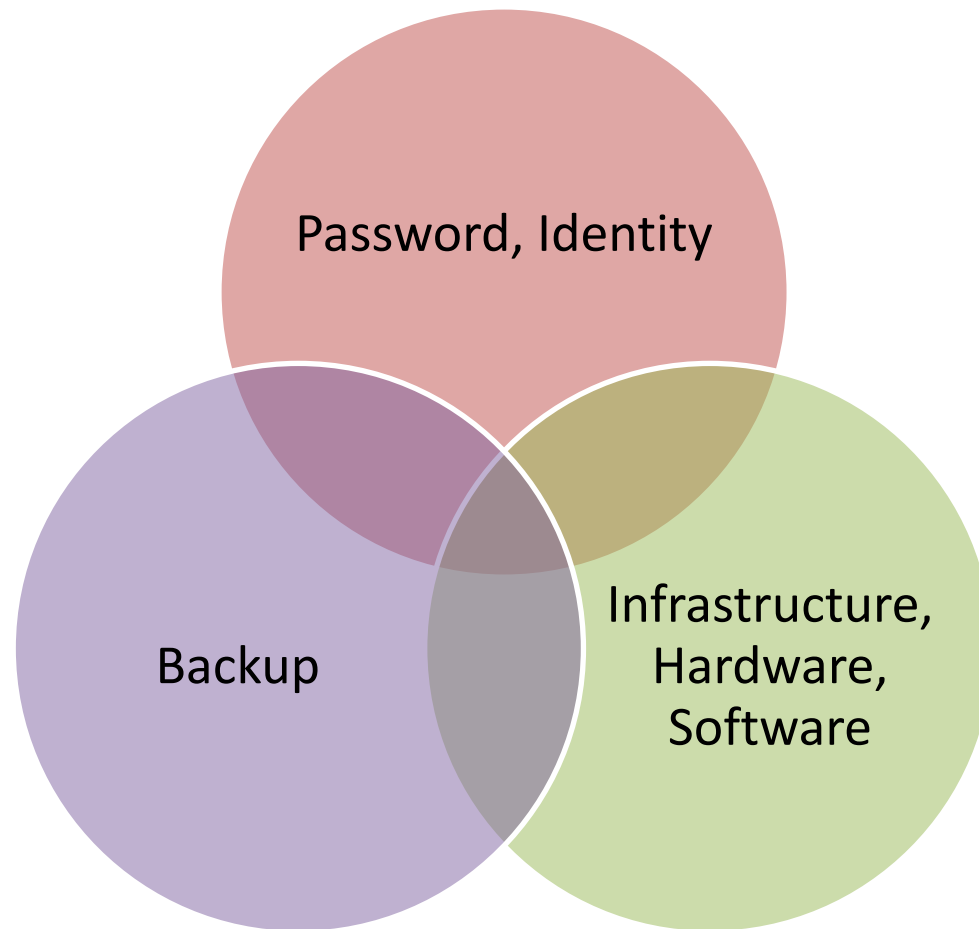
# Prinsip asas keselamatan ICT

1



# Kawalan keselamatan ICT

1



# Dasar Keselamatan ICT v2.0

1



Mesyuarat Eksekutif Universiti (MEU) bersetuju menerima pakai **Dasar Keselamatan ICT V 2.0** Universiti Teknologi MARA berkuatkuasa mulai **1 November 2018**.

**DASAR KESELAMATAN ICT**

Dasar Keselamatan ICT (DKICT) UiTM Versi 2.0 merupakan sebuah dokumen yang **menggariskan peraturan penggunaan aset** dan **kemudahan ICT UiTM** dengan cara yang betul dari aspek keselamatan ICT.

**Penjagaan keselamatan** adalah suatu **proses** yang berterusan.

DKICT UiTM Versi 2.0 diwujudkan untuk memastikan penggunaan sumber dan aset ICT universiti oleh setiap pengguna, dari segi **infrastruktur, sistem aplikasi, kemudahan** serta **data**, adalah mengikut **peraturan dan undang-undang**.

Dasar ini juga menerangkan kepada semua pengguna (warga atau pihak ketiga) di UiTM mengenai **tanggungjawab** dan **peranan** mereka dalam **melindungi aset ICT UiTM**.

Disediakan oleh:  
Bahagian Keselamatan ICT, Jabatan Infostruktur, PPII

**KANDUNGAN DKICT**

- BIDANG 01:** Pembangunan dan Penyelenggaraan Dasar
- BIDANG 02:** Organisasi Keselamatan
- BIDANG 03:** Pengurusan Aset
- BIDANG 04:** Keselamatan Sumber Manusia
- BIDANG 05:** Keselamatan Fizikal dan Persekitaran
- BIDANG 06:** Pengurusan Operasi dan Komunikasi
- BIDANG 07:** Kawalan Capaian
- BIDANG 08:** Laman Web dan Tapak Hosting
- BIDANG 09:** Perolehan, Pembangunan dan Penyelenggaraan Sistem
- BIDANG 10:** Pengurusan Pengendalian Insiden Keselamatan
- BIDANG 11:** Pengurusan Kesenambungan Perkhidmatan
- BIDANG 12:** Pematuhan
- BIDANG 13:** Pemakaian Dasar, pekeliling dan Garis Panduan ICT Semasa Peringkat Kebangsaan

Sila imbas QR Code untuk muat turun Dasar Keselamatan ICT UiTM.

- Sebagai rujukan utama mengenai Keselamatan ICT
- Supaya staf UiTM dan pihak ketiga
  - Patuh dengan peraturan Dasar Keselamatan ICT
  - Menggunakan kemudahan ICT dengan berhemah
  - Menjaga keselamatan aset ICT

# Dasar Keselamatan ICT v2.0 (samb.)

1

- Objektif
  - Memastikan kelancaran operasi universiti
  - Melindungi kepentingan staf dan sistem aplikasi
  - Memastikan aset ICT terlindung daripada ancaman
  - Mencegah kes-kes penyalahgunaan

## Dasar Keselamatan ICT v2.0 (samb.)

1

- <https://ppii.uitm.edu.my> > Muat Turun > Dasar dan Pekeliling ICT > Dasar, Garis Panduan dan MPK



Link tersebut adalah betul dan boleh digunakan semasa nota ini disediakan.



UNIVERSITI  
TEKNOLOGI  
MARA

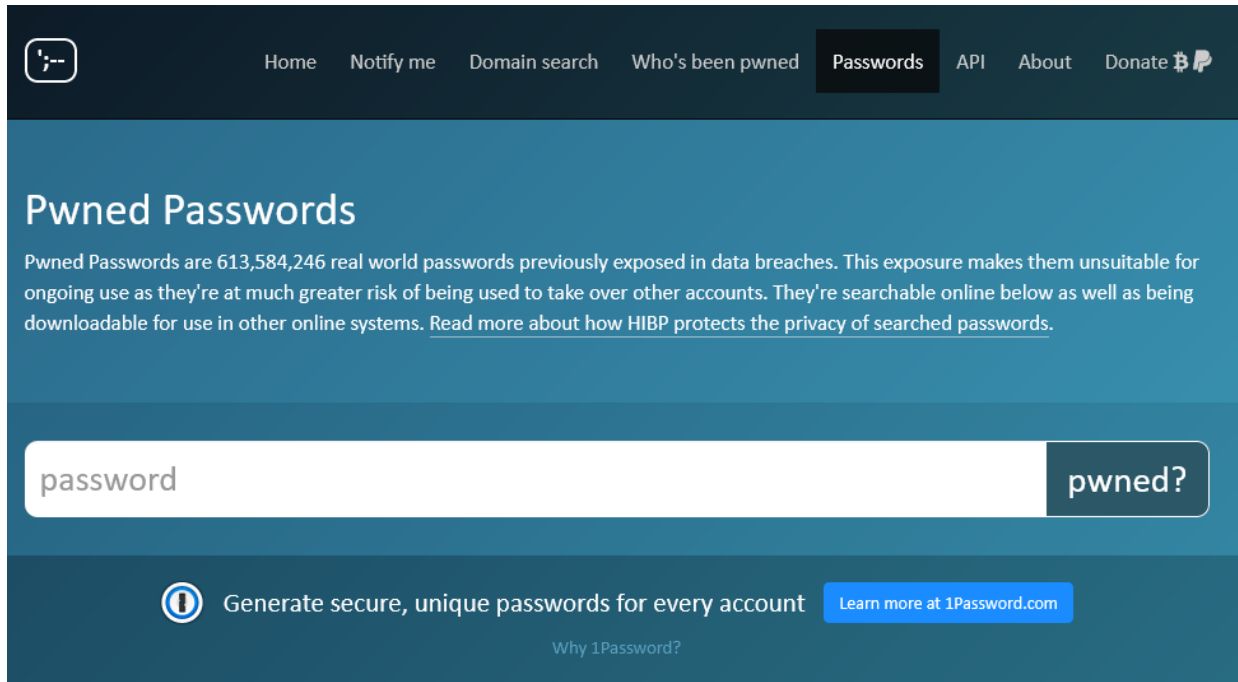
2

# Akses Keselamatan



# Kata Laluan

2



Home Notify me Domain search Who's been pwned Passwords API About Donate

## Pwned Passwords

Pwned Passwords are 613,584,246 real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. [Read more about how HIBP protects the privacy of searched passwords.](#)

 pwned?

<https://haveibeenpwned.com/Passwords>

Link tersebut adalah betul dan boleh digunakan semasa nota ini disediakan.

## Kata Laluan (samb.)

# 2

- Mesti melebihi 8 aksara yang mengandungi:
  - Huruf besar, huruf kecil
  - Nombor
  - Simbol

Atau

- Menggunakan passphrase
- Contoh : Sayasukamakannasikerabu!

## Kata Laluan (samb.)

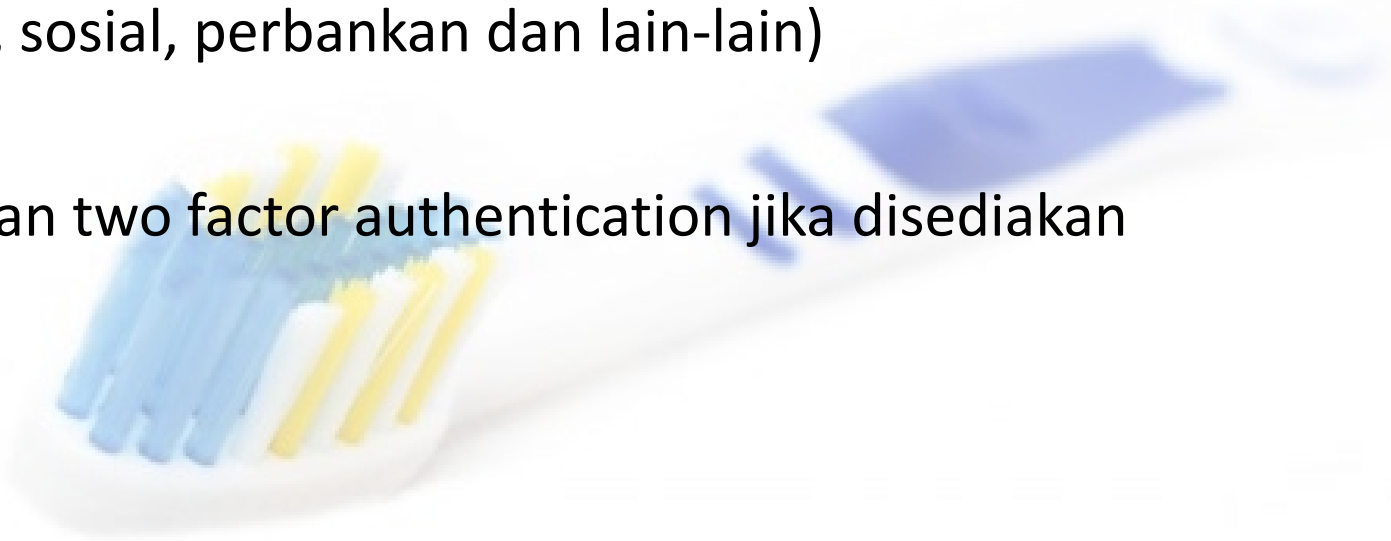
# 2

- Kata laluan ibarat Berus Gigi
  - Perlu kerap ditukar
  - Jangan kongsi kata laluan dengan orang lain
- Gunakan kata laluan berbeza untuk aplikasi berbeza
- Contoh:
  - Olymp!cJapan2021@facebook
  - Olymp!cJapan2021@xyzbank
  - Olymp!cJapan2021@gmail

## Kata Laluan (samb.)

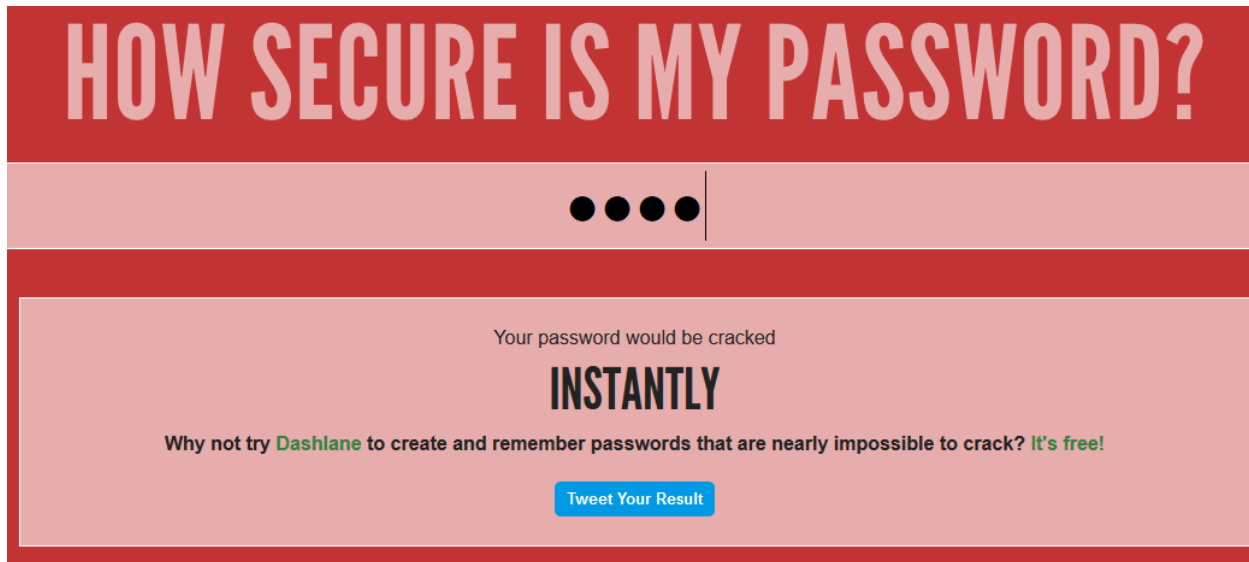
# 2

- Gunakan akaun emel berbeza untuk setiap aspek kehidupan (rasmi, sosial, perbankan dan lain-lain)
- Gunakan two factor authentication jika disediakan



## Kata Laluan (samb.)

2



HOW SECURE IS MY PASSWORD?

●●●●

Your password would be cracked  
**INSTANTLY**

Why not try **Dashlane** to create and remember passwords that are nearly impossible to crack? **It's free!**

[Tweet Your Result](#)



<https://howsecureismypassword.net>

Link tersebut adalah betul dan boleh digunakan semasa nota ini disediakan.

## Web SSO

# 2

- Kemudahan warga UiTM untuk mengakses aplikasi UiTM dalam 1 portal (<https://sso.uitm.edu.my>)
- Pengguna perlu gunakan 1 akaun untuk mengakses
  - FinePortal
  - Staff Portal
  - Dan banyak lagi
- Kata laluan WebSSO akan diminta untuk ditukar setiap 6 bulan



UNIVERSITI  
TEKNOLOGI  
MARA

3

# Keselamatan Maklumat

# Data adalah Aset

3

What is your data worth?

DEMOGRAPHICS FAMILY & HEALTH PROPERTY ACTIVITIES CONSUMER

Data brokers scour public documents, such as birth records and motor vehicle reports, to compile basic data about individuals. It is likely they already know you:

- Age
- Gender
- ZIP code
- Ethnicity
- Education level

Are you a millionaire?

No  
 Yes

What is your job?

Not selected

Are you engaged to be married?

Yes  
 No

**\$0.007**  
Current value of my data

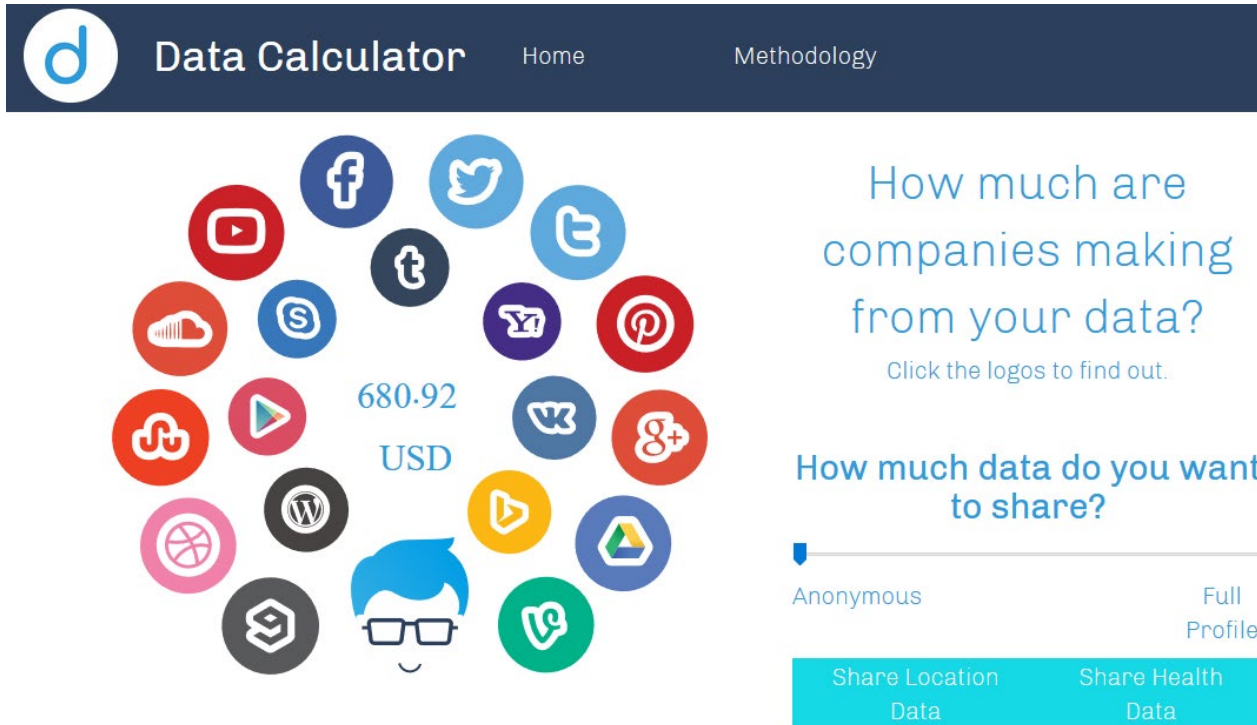


<https://ig.ft.com/how-much-is-your-personal-data-worth/>

Link tersebut adalah betul dan boleh digunakan semasa nota ini disediakan.



## Data adalah Aset (samb.)



The screenshot shows the 'Data Calculator' website. The header includes a logo 'd' and navigation links for 'Home' and 'Methodology'. The main content area features a circular arrangement of social media and service icons (Facebook, Twitter, YouTube, LinkedIn, etc.) with a central value of '680.92 USD'. Below this, there are two questions: 'How much are companies making from your data?' and 'How much data do you want to share?'. The second question has a slider set to 'Anonymous' and two buttons: 'Share Location Data' and 'Share Health Data'. A QR code is located on the right side of the interface.

<https://calc.datum.org/>

Link tersebut adalah betul dan boleh digunakan semasa nota ini disediakan.

# Data adalah Aset (samb.)

3

## Dark Web Price Index 2021



Zachary Ignoffo  
Updated: 1 June 2021



Miklos Zoltan  
Fact-checked by

2 Comments

You wouldn't know it by watching the news, with everything that's been happening surrounding the pandemic and global politics, but up until this point, 2020 has been one of the worst years for cyber attacks.

Notable corporations and organizations like NASA, McDonald's, Microsoft, T-Mobile, Lockheed Martin, even cybersecurity companies FireEye and SolarWinds have all been victims to serious breaches in 2020 alone.

Where does all of this leaked information end up? For sale on the Dark Web of course. We investigated how the Dark Web market has changed since our previously reported [Dark Web Price Index 2020](#), so you can understand what your personal information is worth and why you should protect it.

*Info reflects data collected on May 9 2021.*



<https://www.privacyaffairs.com/dark-web-price-index-2021/>

Link tersebut adalah betul dan boleh digunakan semasa nota ini disediakan.

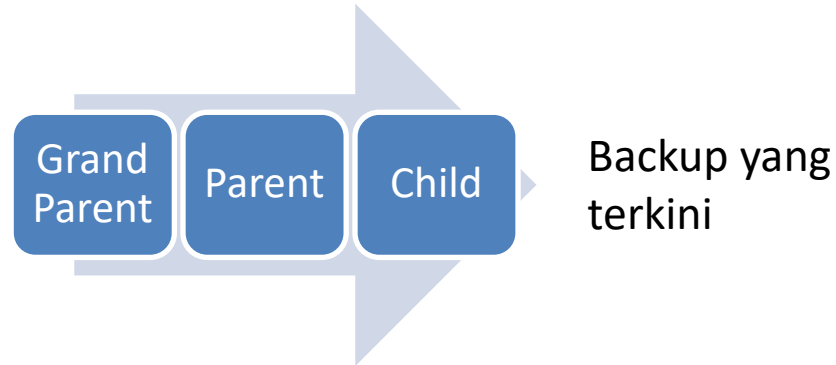
## Back Up

# 3

- Back Up adalah salinan sumber yang boleh digunakan untuk menggantikan sumber utama yang gagal atau terhapus

## Back Up (samb.)

- Sekurang-kurangnya 3 generasi Back Up perlu diadakan



- Sekiranya berlaku masalah teknikal, back up ini sedia untuk digunakan

- Penggunaan perkhidmatan Cloud sebagai alternatif penyimpanan maklumat adalah digalakan.
- Antara perkhidmatan Cloud yang sedia ada dilanggan oleh UiTM adalah
  - **Microsoft Office OneDrive**
  - **Google Drive**
- Pengaktifan akaun Microsoft Office 365 menggunakan domain **<nama>@staf.uitm.edu.my** diperlukan



UNIVERSITI  
TEKNOLOGI  
MARA

4

# Keselamatan Emel

# Keselamatan Emel

# 4

- Terdapat 2 jenis ancaman keselamatan emel
  - Emel SCAM (penipuan)
  - Emel Ugutan

## Ciri-ciri emel SCAM

# 4

- Menceritakan perkara yang meminta penerima mengambil tindakan segera
- Selalunya emel dilampirkan dengan Attachment yang mengandungi malware dan/atau url link
- Teknik ini juga digunakan untuk memancing mangsa untuk memberikan kata laluan (teknik phishing)



# Ciri-ciri emel SCAM (samb.)



LHDN MALAYSIA

Dear Valued Taxpayer,

Please be informed that the INLAND REVENUE BOARD OF MALAYSIA has concluded account audit for the previous tax quarter and after a critical review of your tax you are qualified for an income tax refund of RM 2,000.00 which is your accrued tax excesses till date.

Kindly click below to submit a refund request to enable us process and remit your refunds into your bank account.

[Submit Request](#)

**Note:** Mobile verification is a mandatory step to ensure the accuracy of your account against tax refund fraud, kind of con

You are advised to complete the request payment of your refunds as the same

- Fail to verify your mobile number
- Submit inaccurate/incomplete a

Attention: If you have received this "Not spam" in ot

185.70.11.230/...comcomco/wp-include/hasil/hs.php?url=www.ha

185.70.11.230/...comcomco/wp-include/hasil/hs.php?url=www.hasil.gov.my

AmBank Group

Welcome to our AmOnline Income Tax Refund

Sumber

<https://www.mycert.org.my/en/services/advisories/mycert/2016/main/detail/1195/index.html>

## Ciri-ciri emel Ugutan

# 4

- Memaklumkan bahawa rahsia anda bakal terbongkar jika tidak membayar sejumlah wang.
- Meminta wang dalam bentuk cryptocurrency dalam tempoh terhad

# Ciri-ciri emel Ugutan (samb.)

# 4

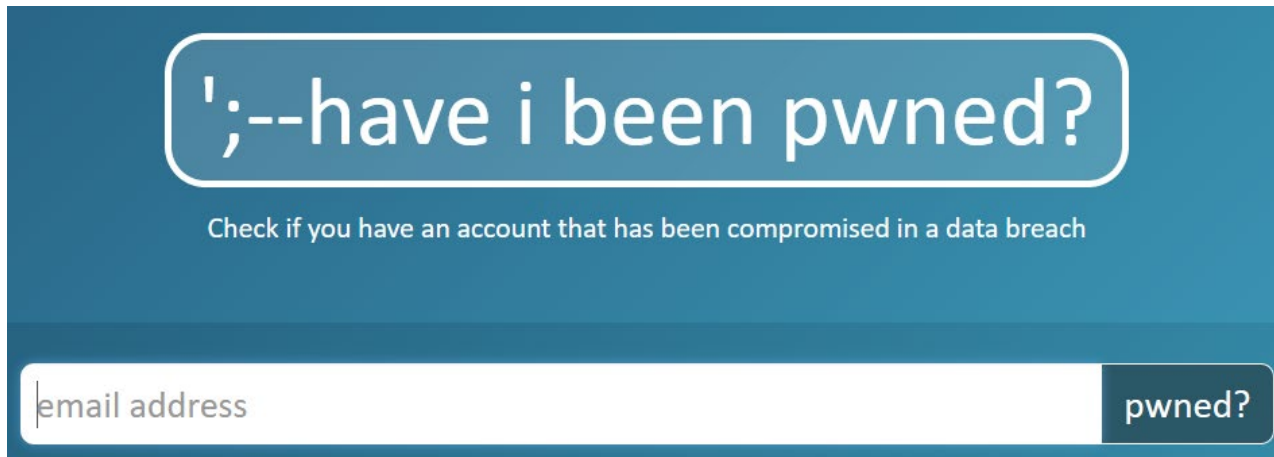
From: "Charlene Kenyon" <[REDACTED]@outlook.com>  
To: [\[REDACTED\]@salam.uitm.edu.my](mailto:[REDACTED]@salam.uitm.edu.my)  
Date: [REDACTED] Nov 2018  
Subject: [REDACTED] - [REDACTED]

---

Hello there, I know the too dirty secrets of your life. I will not tell you just what exactly I know, I've all the details with me. To demonstrate this, just let me reveal you that one of your security passwords is actually [REDACTED]. Send me \$9000 via Bitcoin to the address [REDACTED] within the next 49 hours. Ok, i will make one thing very clear, that I will destroy your life totally if I do not get the payment. When I get the payment, I'll remove every details I've with me, and I will disappear for good . and you will definitely don't ever hear a thing from myself. This is the first and also last e-mail from me as well as the offer is non negotiables, so do not answer to this email.

## Semakan emel

4



I;--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address pwned?



<https://haveibeenpwned.com>

Link tersebut adalah betul dan boleh digunakan semasa nota ini disediakan.

## Tindakan

# 4

- Membuat aduan melalui Sistem Aduan ICT (<https://units.uitm.edu.my>)
- Menghantar salinan emel kepada Bahagian Keselamatan ICT
- Jangan mengambil tindakan untuk membalas atau mengikut kehendak pengirim emel tersebut

## Tips keselamatan Emel

# 4

- Gunakan akaun emel berbeza untuk setiap aspek kehidupan
- Contoh:
  - Emel rasmi
  - Emel urusan perbankan
  - Emel sosial



UNIVERSITI  
TEKNOLOGI  
MARA

5

# Penyelenggaraan Keselamatan ICT

---

# Penyelenggaraan

# 5

- Windows Update
  - Pengguna perlu tahu pentingnya Windows Update
  - Windows Update membolehkan patch dilakukan
  - “Patch Tuesday” merupakan hari Selasa kedua dalam bulan semasa untuk Windows Security Patch
- Anti Virus
  - Pastikan definition antivirus dikemaskini dan yang terkini
  - Kegagalan perisian mendapatkan definition terkini mengakibatkan antivirus tidak dapat mengenalpasti jenis virus baru





UNIVERSITI  
TEKNOLOGI  
MARA

6

# Aduan Keselamatan ICT

---

- <https://units.uitm.edu.my>
- Kategori Aduan di bawah Keselamatan ICT
  - Antivirus
  - Domain \*.uitm.edu.my
  - Insiden
  - SMTP Gateway
  - SSL/TLS
  - Web Application Firewall (WAF)
  - Web SSO

Category* :	-CHOOSE CATEGORY-
Sub Categories* :	-CHOOSE CATEGORY- APLIKASI - TURNITIN IP TELEPHONY (UITM PUNCAK ALAM)
Details* :	KESELAMATAN - ANTIVIRUS KESELAMATAN - DOMAIN *.UITM.EDU.MY KESELAMATAN - INSIDEN KESELAMATAN - SMTP GATEWAY
Attachment :	KESELAMATAN - SSL/TLS KESELAMATAN - WEB APPLICATION FIREWALL (WAF) KESELAMATAN - WEB SSO

## Tips keselamatan ICT

- Sistem Maklumat PDRM – semak akaun bank / no. Telefon SCAM



<https://ccid.rmp.gov.my/semakmule>

Link tersebut adalah betul dan boleh digunakan semasa nota ini disediakan.

## Tips keselamatan ICT (samb.)

# 6

- Laporkan isu keselamatan siber kepada Cyber999
  - Telefon: 1-300-88-2999
  - Emel: [cyber999@cybersecurity.my](mailto:cyber999@cybersecurity.my)
  - Mobile Apps: Cyber999



UNIVERSITI  
TEKNOLOGI  
MARA

**TERIMA KASIH**