Digital @USM
PUSAT TRANSFORMASI DIGITAL
USM KAMPUS KEJURUTERAAN
TUANKU SYED SIRAJUDDIN

BIT OF BYTE MAGAZINE

EDISI 2026

BYTE BACK THE SCAMMERS

AWARE
PREVENT
PROTECT
RESPOND

Lindungi diri daripada penipuan digital

REAL
PEOPLE
REAL
THREATS
REAL
SOLUTIONS

SAME
TECH
BIGGER
SAFER
PEOPLE

A
SAFER
BRIGHTER
DIGITAL
TOMORROW

KNOW
PREVENT
ACT
A SAFER
TOMORROW

STAY ALERT
STAY SMART
STAY SAFE

SCAM

URGENT!
Verify your account now!

You've won a prize! Claim now!

Transfer now or lose access!

FAKE OFFERS
PHISHING
IDENTITY THEFT
ONLINE FRAUD
DATA BREACH
MONEY TRAP

Kenal pasti scam

WASPADA DENGAN TANDA-TANDA PENIPUAN DIGITAL.

Jangan klik pautan mencurigakan

PAUTAN PALSU BOLEH MENCURI DATA ANDA.

Semak sebelum bayar

PASTIKAN MAKLUMAT DAN PENERIMA SAHIH.

Lapor & bertindak segera

JANGAN BERDIAM, BERTINDAK SEKARANG.

PEOPLE
AWARENESS
TECHNOLOGY
SAFER COMMUNITIES

Bijak digital, selamat online.

SMALL
ACTIONS
MAKE A
SAFER WORLD

BIT OF BYTE MAGAZINE

SIDANG PENGARANG

Ketua Editor
Pn. Mashithah Bt. Md Hasim

Ahli
Pn. Hjh. Umul Hapsah Bt. Mohamad
En. Mohamad Khairi B. Osman
En. Suhaimi B. Saibon
Tn. Hj. Mohd Kusairay B. Musa
Pn. Nurzalina Bt. Nordin
Tn. Hj. Mohamed Amir Husaini B. Abd Hamid
Pn. Shariza Bt. Sharuddin
Pn. Shariza Bt. Shaari



Penaung
Tn. Hj. Mazlifendirizan B. Md Rejab

Senireka & Grafik
En. Hishammudin B. Endan
Pn. Hjh. Sharifah Shakila Bt. Md Saad



PENULIS JEMPUTAN

En. Muhammad Rizal Bin Mohamad Amin
En. Mahadi Bin Yusof
Ts. Zaiyana Binti Mohamed Hussain

Digital @USM
PUSAT TRANSFORMASI DIGITAL
USM KAMPUS KEJURUTERAAN
TUANKU SYED SIRAJUDDIN

BIT OF BYTE
MAGAZINE

KANDUNGAN

01 Dari Meja Ketua Editor

02 Dari Meja Timbalan Pengarah

03 DECEPTION: Seni Tipu Daya dalam Dunia Digital

04 Menggunakan AI untuk Melawan AI: Alat Baharu bagi Mengesan Email Penipuan

05 Scam 4.0: Bila AI Digunakan Untuk Menipu (Deepfake)

06 Integriti Data Dan Risiko Halusinasi Dalam AI

07 Teka Silang Kata

08 War Of The World

09 Transformasi Digital USM: Memperkasa Warga Akademik Dan Pengurusan Profesional Dengan Google Gemini AI Pro

10 Digital Trust Under Attack: Melawan Ancaman Scam & Penipuan Siber

11 Mereka Tidak Menggodam Sistem, Mereka Menggodam Manusia

12 Klik, Percaya, Lesap: Taktik Licik Scammer Masa Kini

13 Memperkasa Pertahanan Siber: Bagaimana USM Menguasai Piawaian Keselamatan Maklumat Bertaraf Dunia

14 Senyum IT

15 Siapa Sebenarnya Scammer?

16 Scammer di IPT

17 Panduan Menghadapi Ancaman Scammer

18 BitLocker: Pelindung Data atau Punca Masalah?

19 Simple Shaz: Excel Flash Fill

20 Dari Isyarat Otak ke Pergerakan Kaki: Kisah Teknologi Cybernic Voluntary Control System (CVCS)



MASHITHAH MD HASIM
Ketua Editor | Majalah Bit of Byte 2026

KATA ALU-ALUAN KETUA EDITOR

"Byte Back the Scammers"

- **Salam Sejahtera dan Salam Digital kepada Para Pembaca yang Dihormati,**

  Selamat datang ke lembaran edisi terbaharu majalah Bit of Byte 2026!

  Sebagai ketua editor, saya rasa amat teruja dan bangga dapat menyapa anda semua menerusi naskhah kali ini. Tahun 2026 menyaksikan lanskap teknologi yang semakin canggih namun di sebalik kemajuan pesat ini tersembunyi bayang-bayang ancaman yang kian licik. Atas kesedaran inilah, kami mengetengahkan tema yang amat mendesak dan relevan: ***"Byte Back the Scammers".***

  Naskhah ini dibawakan khas bukan sekadar sebagai wadah maklumat malah sebagai perisai digital untuk kita bersama-sama bangkit melawan, mendidik diri dan mempertahankan hak serta keselamatan kita di alam maya. Setiap bait kata dan rencana yang digarap adalah seruan untuk kita tidak lagi menjadi mangsa sebaliknya bersatu membendung jenayah siber yang kian berleluasa.

- **Setinggi-tinggi Penghargaan**

  Kejayaan penerbitan majalah ini sudah tentu tidak akan menjadi kenyataan tanpa usaha gigih dan komitmen yang tidak berbelah bahagi daripada pelbagai pihak.

  "Kejayaan sebuah naskhah hebat tidak pernah lahir dari usaha seorang diri melainkan daripada gabungan ilham, peluh dan semangat sebuah pasukan."

  Secara peribadi, saya ingin merakamkan setinggi-tinggi penghargaan dan ucapan terima kasih kepada:

  - **Ahli Jawatankuasa (JK) Editorial BOB:** Terima kasih atas keringat, idea kreatif dan kesabaran meniti setiap fasa penerbitan. Daripada susun atur grafik, suntingan teks hinggalah ke proses penyemakan terakhir, kalian adalah tulang belakang sebenar majalah ini.
  - **Para Penulis Artikel:** Terima kasih kerana sudi menyumbang idea dan penulisan, berkongsi ilmu dan melakukan kajian mendalam bagi melahirkan rencana yang sarat dengan maklumat mutakhir serta impak tinggi. Dedikasi kalian dalam membongkar taktik penipuan digital amat saya kagumi.

Harapan Kami

Akhir kata, saya berharap agar naskhah "Byte Back the Scammers" ini dapat memberi manfaat yang bermakna, menyuntik kesedaran dan mengasah kepekaan kita dalam melayari dunia digital yang serba mencabar ini. Selamat membaca dan mari kita bersama-sama memperkasakan diri kerana keselamatan digital bermula daripada kita!



Kepercayaan Digital Dalam Era Kecerdasan Buatan

Membina asas integriti, ketahanan keselamatan siber dan budaya digital bertanggungjawab di Universiti Sains Malaysia.



EN. MAZLIFENDIRIZAN B. MD REJAB
TIMBALAN PENGARAH
Pusat Transformasi Digital
Kampus Kejuruteraan Tuanku Syed Sirajuddin
Universiti Sains Malaysia

"Teknologi sentiasa bersifat neutral. Nilai sesuatu teknologi bergantung kepada bagaimana manusia memilih untuk menggunakannya."

Transformasi digital kini bukan lagi sekadar mengenai penggunaan teknologi baharu atau pendigitalan proses kerja. Kita telah melangkah ke satu fasa yang jauh lebih mencabar apabila kecerdasan buatan (*Artificial Intelligence - AI*) mula menjadi sebahagian daripada rutin harian kita.

AI membantu menghasilkan kandungan, menganalisis data, mempercepat penyelidikan, meningkatkan produktiviti serta menyokong proses membuat keputusan. Namun, dalam masa yang sama, teknologi yang sama juga boleh dimanipulasi untuk menyebarkan maklumat palsu, menghasilkan kandungan manipulatif, melaksanakan serangan kejuruteraan sosial dan memperdaya pengguna yang kurang berwaspada.

Inilah hakikat dunia digital hari ini. Cabaran terbesar yang sedang kita hadapi bukanlah kekurangan teknologi, tetapi bagaimana membina dan mengekalkan **kepercayaan digital** ***(digital trust)*** dalam setiap aspek penggunaan teknologi tersebut di universiti kita.

"Cabaran terbesar kita bukanlah kekurangan teknologi, tetapi membina kepercayaan digital dalam setiap aspek penggunaannya."



PRINSIP TERAS Integriti • Keselamatan • Kepercayaan

Kepercayaan digital tidak boleh dibina hanya melalui pemasangan perisian keselamatan, firewall atau teknologi perlindungan siber yang canggih. Sebaliknya, ia bermula daripada budaya organisasi yang menghargai integriti, tanggungjawab dan literasi digital.

Setiap warga universiti mempunyai peranan penting dalam memastikan data dipelihara dengan baik, maklumat disahkan sebelum dikongsi, identiti digital dilindungi dan teknologi AI digunakan secara beretika serta bertanggungjawab.

EKSPLOITASI & ANCAMAN SIBER ALAF BAHARU

Penjenayah siber kini tidak lagi sekadar menyerang kelemahan kod sistem komputer, sebaliknya mengeksploitasi psikologi emosi dan kepercayaan manusia:

- ⚠ DEEPFAKE
- ⚠ PHISHING
- ⚠ MALWARE
- ⚠ SOCIAL ENGINEERING
- ⚠ CYBER SCAM



PERINGATAN KESELAMATAN Kenal Pasti Taktik Penipuan Digital Terkini

Justeru, tema yang diketengahkan dalam keluaran *Bit of Byte* kali ini amat signifikan dalam menyuntik kepekaan berterusan agar ancaman ini dapat dipatahkan pada peringkat awal.

DIGITAL TRANSFORMATION USM

Bersama Memacu Transformasi Digital Yang Selamat, Mampan dan Berintegriti

MISI APEX



KERANGKA TERAS USM

Perbincangan mengenai ancaman siber, manipulasi AI dan eksploitasi data bukan bertujuan menimbulkan kebimbangan atau rasa panik. Sebaliknya, ia bertujuan meningkatkan kesedaran bahawa ancaman siber hari ini semakin kompleks, lebih pintar dan semakin sukar dibezakan daripada realiti sebenar.

Dalam masa yang sama, kita juga berbangga berkongsi pelbagai inisiatif strategik positif yang sedang giat dilaksanakan oleh USM. Ini termasuklah pemerkasaan penggunaan **Google Gemini AI Pro** secara berstruktur, pengukuhan standard tadbir urus keselamatan maklumat bertaraf antarabangsa (ISO/IEC 27001), serta penyediaan infrastruktur awan yang selamat bagi melonjakkan kecekapan aktiviti penyelidikan, pentadbiran dan pembelajaran.

TUNJANG NILAI PEMIMPIN DIGITAL

"Kejayaan sesebuah universiti dalam era digital tidak lagi diukur semata-mata pada bilangan sistem yang dibangunkan atau kecanggihan teknologi yang dimiliki, sebaliknya pada kematangan warganya membuat pertimbangan beretika."

Semua usaha ini mencerminkan komitmen jitu universiti untuk memastikan agenda transformasi digital berlaku secara menyeluruh, inklusif, selamat dan mampan demi kebaikan warga kampus sejagat.

4 Tonggak Ketahanan Ekosistem Digital USM

01 Literasi Kritis

Melahirkan warga yang tidak menelan bulat-bulat maklumat siber serta bijak menyaring deepfake.

02 Tadbir Urus Data

Mematuhi garis panduan keselamatan data ketat bagi menjaga privasi maklumat universiti.

03 Etika AI Proaktif

Mengoptimumkan Google Gemini AI Pro dan alat automasi untuk penyelidikan berintegriti.

04 Budaya Berwaspada

Mengekang kejuruteraan sosial dan taktik scam dengan pengesahan identiti berganda.

Saya percaya bahawa kejayaan sebenar amat bergantung kepada sejauh mana kita mampu melahirkan warga kampus yang celik digital, berfikiran kritis, teguh berintegriti dan berkeupayaan membuat pertimbangan yang bijaksana ketika mendepani ledakan teknologi baharu.

Saya berharap setiap artikel yang disajikan dalam keluaran *Bit of Byte* ini dapat dimanfaatkan sepenuhnya sebagai sumber ilmu, pencetus inspirasi dan kompas panduan dalam memperkukuh daya tahan digital kita bersama.

Marilah kita terus membudayakan pembelajaran sepanjang hayat, mengamalkan penggunaan teknologi secara beretika dan bersama-sama membina ekosistem digital yang selamat, dipercayai serta memberi impak positif kepada seluruh warga universiti.

Selamat membaca.

DECEPTION:

SENI TIPU DAYA DALAM DUNIA DIGITAL

Oleh: Mazlifendirizan Md Rejab

Dalam dunia digital hari ini, scam bukan lagi sekadar panggilan telefon mencurigakan atau mesej SMS yang pelik. Ia telah berkembang menjadi satu bentuk jenayah moden yang tersusun, profesional dan sangat meyakinkan.

Dari love scam, pelaburan palsu, phishing, sehinggalah kepada eksploitasi sistem kewangan, scammer kini menggunakan teknologi dan psikologi manusia sebagai senjata utama.

Apa yang lebih membimbangkan, scam tidak lagi mensasarkan golongan tertentu sahaja. Mangsa terdiri daripada pelajar, pensyarah, pegawai kerajaan, profesional malah individu yang celik teknologi.



TAHUKAH ANDA?

Malaysia merekodkan lebih

66,000

kes penipuan dalam talian dengan kerugian hampir

RM3 BILION

pada tahun 2025 sahaja.

Bayangkan apa yang boleh dilakukan dengan RM 3 bilion tersebut — ribuan rumah mampu milik, hospital, sekolah atau bantuan kepada jutaan rakyat.

24 = RM8 JUTA SEHARI

= RM95 SESAAT

MENGAPA SCAM BEGITU BERKESAN?

Persoalannya, mengapa scam begitu berkesan?

Jawapannya terletak pada konsep "deception" atau tipu daya. Scammer tidak semestinya perlu menggodam sistem komputer. Sebaliknya, mereka menggodam cara manusia berfikir.

Teknik seperti sense of urgency, manipulasi emosi, penyamaran identiti dan janji keuntungan cepat digunakan untuk mempengaruhi mangsa membuat keputusan tanpa berfikir panjang.



SENJATA TIPU DAYA SCAMMER

SENSE OF URGENCY

Mendesak mangsa bertindak segera supaya tidak sempat berfikir atau semak kesahihan.

MANIPULASI EMOSI

Memainkan perasaan seperti takut, simpati, cinta atau tamak untuk mengawal keputusan mangsa.

PENYAMARAN IDENTITI

Menyamar sebagai individu, organisasi atau agensi yang dipercaya untuk mendapatkan kepercayaan.

JANJI KEUNTUNGAN CEPAT

Tawaran pelaburan palsu dengan keuntungan tinggi dalam masa singkat untuk memancing mangsa.

> Scam bukan serangan terhadap teknologi semata-mata, tetapi serangan terhadap psikologi manusia.

SCAMMER MODEN:
BEROPERASI SEPERTI ORGANISASI



Menariknya, konsep penipuan ini bukanlah sesuatu yang baru. Sejak zaman Nabi Adam AS, tipu daya telah digunakan untuk mempengaruhi manusia membuat keputusan yang salah. Dalam sejarah para nabi juga wujud penipuan dalam bentuk timbangan tidak jujur, janji palsu dan manipulasi kepercayaan. Bezanya hari ini, teknologi menjadikan scam lebih pantas, lebih luas dan lebih sukar dikesan.

Scammer moden beroperasi seperti sebuah organisasi. Mereka mempunyai skrip, pusat panggilan, akaun keldai dan rangkaian transaksi rentas negara. Wang yang dicuri dipindahkan dalam beberapa minit melalui pelbagai akaun sebelum akhirnya lesap melalui crypto atau transaksi luar negara.

BAGAIMANA SCAM BEROPERASI?

1	2	3	4	5	6
MENGHUBUNGI MANGSA	**MEMBINA KEPERCAYAAN**	**MEMANIPULASI MANGSA**	**MEMINTA TINDAKAN**	**MEMINDAH DANA**	**LESAP**
Melalui panggilan, SMS, media sosial atau emel.	Menggunakan skrip profesional dan identiti palsu.	Menggunakan emosi, sense of urgency atau janji keuntungan.	Minta pindahan wang. Kongsikan OTP atau klik pautan.	Wang dipindahkan ke akaun keldai berlapis-lapis.	Dana dikeluarkan melalui crypto atau transaksi luar negara.

FAKTA MENARIK

- Scammer kini menggunakan AI untuk meniru suara, menjaga dokumen palsu dan mencipta laman web palsu yang sangat meyakinkan.
- Pusat panggilan scam beroperasi 24/7 dengan pasukan yang terlatih.
- Kerugian bukan hanya wang, tetapi juga trauma emosi dan masa.



LINDUNGI DIRI,
LINDUNGI MASA DEPAN

Namun begitu, pengguna masih mempunyai pertahanan paling penting iaitu kesedaran. Amalkan langkah asas berikut setiap hari:

JANGAN PANIK ATAU TERBURU-BURU
Ambil masa untuk berfikir dan semak kesahihan sebelum bertindak.

JANGAN KLIK PAUTAN YANG MENCURIGAKAN
Pautan palsu boleh mencuri maklumat anda.

JANGAN SESEKALI BERKONGSI OTP ATAU MAKLUMAT PERBANKAN
Bank tidak akan meminta maklumat sensitif melalui telefon atau mesej.

SEMAK NOMBOR DAN IDENTITI MELALUI SALURAN RASMI
Hubungi organisasi melalui nombor rasmi mereka.

DAPATKAN PANDANGAN KEDUA
Berbincang dengan rakan atau keluarga sebelum membuat transaksi.

LAPORKAN SEGERA
Laporkan kepada bank atau NSRC (997) sekiranya anda menjadi mangsa.



> Hakikatnya, scammer hanya memerlukan satu perkara daripada kita iaitu “kepercayaan”.
>
> Oleh itu, dalam era digital ini bukan sahaja sistem yang perlu dilindungi, tetapi juga cara kita berfikir.



BYTE BACK
THE SCAMMERS

Menggunakan AI untuk Melawan AI: Alat Baharu bagi Mengesan Email Penipuan

Oleh : WAN AHMAD SARBINI BIN WAN MOHD ALI



Bayangkan anda menerima emel daripada ketua jabatan atau rakan sekerja dengan gaya bahasa yang sangat sempurna dan profesional, malah menyentuh topik yang memang sedang anda kerjakan. Tiada lagi kesalahan ejaan yang pelik atau ayat Google Translate yang dulunya menjadi tanda amaran utama scammer. Selamat datang ke era penipuan Siber 2.0, di mana Kecerdasan Buatan (AI) kini menjadi penulis upahan paling licik buat penjenayah digital.

Namun, jangan panik. Walaupun penjenayah menggunakan AI untuk membina jerat, kita juga mempunyai senjata yang sama hebatnya untuk memotong tali jerat tersebut. "Byte Back" bukan sekadar slogan malah ia adalah strategi untuk kita menggunakan teknologi yang sama canggih bagi melindungi integriti data dan keselamatan organisasi kita.

Evolusi Ancaman: Apabila Scammer Menjadi 'Cerdik'

Dahulu, kita sering diajar untuk mencari kesilapan tatabahasa sebagai petanda emel penipuan. Namun dengan kewujudan Model Bahasa Besar, scammer kini mampu menjana ribuan emel yang disesuaikan mengikut profil mangsa dalam sekelip mata. Teknik Business Email Compromise (BEC) kini lebih sukar dikesan kerana AI mampu meniru gaya penulisan individu tertentu dengan tepat, membuatkan mangsa rasa selamat untuk menekan pautan berbahaya atau memindahkan wang.

Melawan Api dengan Api: Senjata AI Pertahanan

Untuk menangkis serangan ini, sistem keselamatan emel moden kini telah mengintegrasikan AI sebagai perisai utama. Antara teknologi terbaharu termasuklah:

- **Analisis Linguistik AI:** Walaupun teks nampak sempurna, AI pertahanan boleh mengesan ketiadaan sentuhan manusia atau corak sintaksis yang sering dihasilkan oleh mesin yang tidak mampu dikesan oleh mata kasar.

- **Analisis Tingkah Laku Masa Nyata:** Sistem akan menyemak sama ada corak penghantaran emel tersebut selari dengan sejarah komunikasi biasa. Jika ketua anda tiba-tiba menghantar emel mendesak pada jam 3 pagi dengan arahan luar biasa, AI akan segera memberikan amaran.

- **Computer Vision:** AI digunakan untuk melihat laman web di sebalik pautan emel. Ia boleh mengesan perbezaan piksel yang sangat halus antara laman perbankan sebenar dengan laman phishing.

Tips Pantas: Jangan sesekali bertindak atas emel yang meminta tindakan kewangan segera. Gunakan kaedah pengesahan kedua (seperti panggilan telefon atau mesej WhatsApp terus kepada pengirim) untuk memastikan kesahihan arahan tersebut.

Tanggungjawab Manusia di Era Automasi

Walaupun AI pertahanan sangat hebat, benteng terakhir tetap berada di tangan kita sebagai pengguna. Teknologi AI hanyalah alat namun kebijaksanaan kita dalam menilai situasi adalah kunci utama. Kita perlu sentiasa mengemaskini ilmu tentang trend penipuan terkini dan menggunakan semua lapisan perlindungan yang disediakan oleh organisasi, termasuklah Pengesahan Dua Faktor (2FA).

Kesimpulan

Dunia siber adalah medan perang digital yang sentiasa berubah. Dengan mengadopsi alat berasaskan AI untuk mengesan penipuan, kita bukan sahaja bertahan malah kita sedang menghantar mesej jelas kepada scammer: "Kami mempunyai byte yang lebih kuat untuk menggigit kembali." Jangan biarkan teknologi menjadi kelemahan kita sebaliknya jadikannya perisai yang paling ampuh.

Disediakan oleh: Mohd Kusairay Musa

SCAM 4.0

BILA AI DIGUNAKAN UNTUK MENIPU [DEEPFAKE]



AI memudahkan hidup kita, tetapi di tangan penipu, ia menjadi senjata baharu untuk memperdaya dan memanipulasi.

Jangan jadi mangsa seterusnya!

APAKAH ITU DEEPFAKE?

Deepfake ialah teknologi AI yang mampu menghasilkan video, audio atau imej palsu yang kelihatan sangat realistik dengan meniru wajah, suara dan pergerakan seseorang.



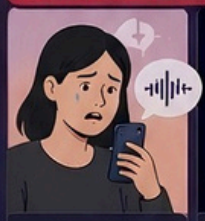


SCAM 4.0: PENIPUAN ERA BAHARU

Penipu menggunakan AI dan deepfake bersama data media sosial untuk memanipulasi emosi dan kepercayaan mangsa.



CONTOH SCAM DEEPFAKE



Suara ahli keluarga ditiru untuk meminta wang kecemasan.



Video palsu tokoh terkenal mempromosikan pelaburan scam.



Wajah individu digunakan dalam video tanpa kebenaran.



Panggilan telefon dengan suara AI yang menyerupai kenalan rapat.

MENGAPA DEEPFAKE SANGAT BERBAHAYA?

1 SUKAR DIBEZAKAN DENGAN REALITI
AI mampu hasilkan kandungan yang sangat meyakinkan.

2 MANIPULASI EMOSI
Penipu gunakan panik, takut dan simpati untuk pengaruhi mangsa.

3 PENYEBARAN SANGAT PANTAS
Video atau audio palsu boleh tular dalam masa singkat.

4 MENJEJASKAN REPUTASI
Boleh digunakan untuk menjatuhkan maruah individu, organisasi atau pemimpin.

TANDA-TANDA DEEPFAKE

- Pergerakan bibir tidak selari dengan suara.
- Ekspresi wajah kelihatan pelik atau terlalu sempurna.
- Kualiti suara kedengaran robotik atau tidak konsisten.
- Video kelihatan kabur pada bahagian tertentu wajah.
- Panggilan kecemasan meminta wang secara tergesa-gesa.
- Individu enggan membuat pengesahan melalui panggilan video sebenar.

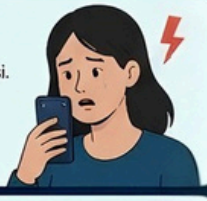


BERWASPADA, BERFIKIR, SAHKAN!

Jangan mudah percaya kepada apa yang dilihat atau didengar.

CARA MELINDUNGI DIRI DARIPDA SCAM AI

1 JANGAN MUDAH PANIK
Scammer sering menggunakan tekanan emosi. Tenangkan diri sebelum membuat sebarang tindakan.



2 BUAT PENGESAHAN
Hubungi semula individu tersebut melalui nombor rasmi atau platform lain.



3 KURANGKAN PENDEDAHAN DATA PERIBADI
Elakkan berkongsi terlalu banyak video, suara dan maklumat peribadi di media sosial secara terbuka.



4 SEMAK KESAHIHAN MAKLUMAT
Jangan mudah percaya kepada video atau audio yang tular tanpa sumber sahih.



5 GUNAKAN KATA LALUAN KESELAMATAN KELUARGA
Wujudkan "kata rahsia keluarga" untuk pengesahan semasa situasi kecemasan.



6 TINGKATKAN LITERASI DIGITAL
Masyarakat perlu dididik tentang ancaman AI dan penipuan digital moden.



TEKNOLOGI TIDAK SALAH, PENGGUNA MENENTUKAN ARAH

AI dicipta untuk membantu manusia. Namun, apabila disalahgunakan, ia boleh menjadi senjata baharu dalam jenayah siber.



Pendidikan digital dan kesedaran keselamatan siber perlu diperkukuhkan bermula dari sekolah, universiti hinggalah ke tempat kerja.

KESIMPULAN

Scam 4.0 membuktikan bahawa penipuan hari ini bukan lagi sekadar mesej palsu atau panggilan telefon biasa. Dengan bantuan AI dan deepfake, scam menjadi lebih licik, realistik dan sukar dikesan.



> "Di era digital, mata boleh tertipu, telinga boleh diperdaya, tetapi ilmu dan kesedaran mampu menjadi pertahanan utama kita."

JADI PENGGUNA BIJAK,
LINDUNGI DIRI, LINDUNGI KELUARGA, LINDUNGI KOMUNITI.

#ByteBackTheScammer #Scam4.0 #CyberSafe #ThinkBeforeYouClick

Oleh: Umul Hapsah Mohamad

Integriti Data dan Risiko Halusinasi dalam Kecerdasan Buatan (AI)

Kecerdasan Buatan (AI) terutamanya Model Bahasa Besar atau Bahasa Inggerisnya dikenali sebagai Large Language Model (LLM) yang digunakan dalam pelbagai aplikasi moden telah merevolusikan cara kita bekerja dan berinteraksi dengan maklumat. Walau bagaimanapun, keupayaan luar biasa AI ini turut membawa cabaran kritikal yang berkisar pada kualiti inputnya dan kebolehpercayaan outputnya. Dua isu utama yang menjadi fokus adalah integriti data dan risiko fenomena yang dikenali sebagai halusinasi AI. Memahami dan mengurus kedua-dua aspek ini adalah penting untuk membina sistem AI yang beretika, berfungsi dan boleh dipercayai. Integriti data merupakan tunjang kebolehpercayaan AI.

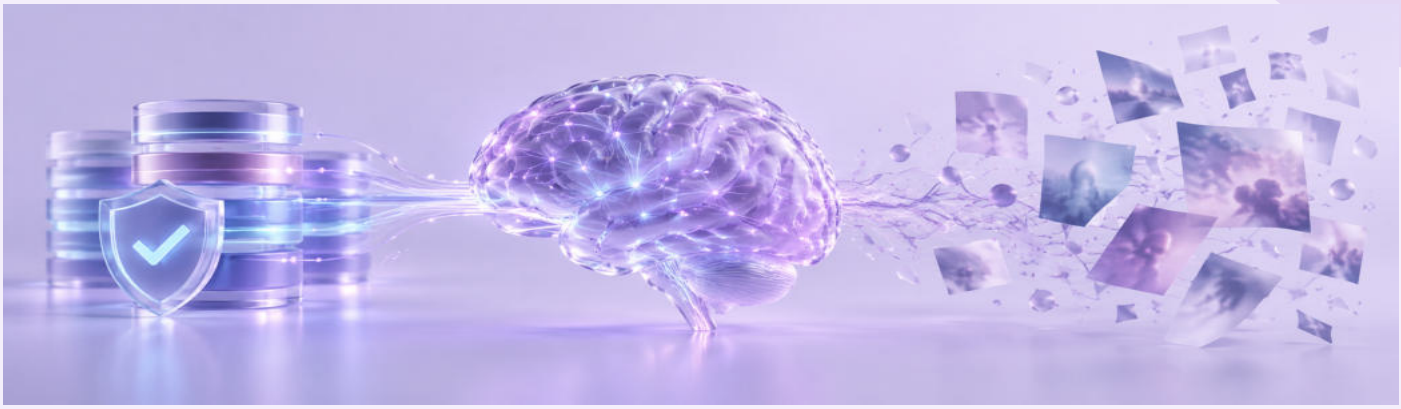




Integriti data ialah asas yang memastikan AI berfungsi secara tepat, adil, telus dan boleh dipercayai. Dalam konteks AI, data bertindak sebagai bahan api yang menjadi sumber utama untuk membuat keputusan dan menjana output. Tanpa integriti data yang kukuh, model AI akan terdedah kepada kecacatan yang serius dan sering dirumuskan seperti pepatah Garbage In, Garbage Out (Sampah Masuk, Sampah Keluar).



Aspek Integriti Data yang Kritikal:



1. **Ketepatan (Accuracy):** Data mesti mencerminkan realiti secara tepat. Kesilapan data input boleh menyebabkan model AI mempelajari korelasi yang salah, menghasilkan keputusan yang cacat atau bias.

2. **Konsistensi (Consistency):** Data perlu seragam merentasi pelbagai sumber. Ketidakselarasan dalam format, unit ukuran atau definisi boleh mengelirukan model.

3. **Kebolehsahihan (Validity):** Data mesti mematuhi peraturan atau had yang telah ditetapkan. Contohnya nilai yang tidak boleh negatif dan format tarikh yang betul.

Apabila integriti data terjejas sama ada melalui pencerobohan siber, ralat input manusia atau pengumpulan data yang tidak sempurna, risiko keputusan AI yang tidak adil atau berbahaya meningkat secara mendadak. Sebagai contoh, sistem AI yang dilatih dengan data yang mengandungi bias sejarah boleh meneruskan dan memburukkan diskriminasi dalam keputusan pengambilan pekerja atau pinjaman.





Risiko Halusinasi dalam AI

Fenomena halusinasi AI berlaku apabila model AI terutamanya LLM, menghasilkan maklumat yang kelihatan meyakinkan dan tepat tetapi sebenarnya adalah salah, direka-reka atau tidak disokong oleh data latihan atau konteks yang diberikan. Model ini tidak berbohong secara sengaja tetapi menghasilkan output berdasarkan corak statistik yang dipelajarinya tanpa benar-benar memahami kebenaran fakta.

Halusinasi berpunca daripada beberapa faktor utama:

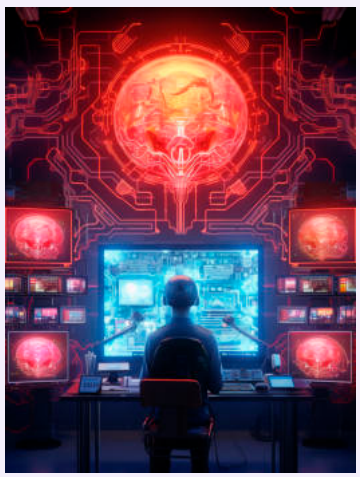
> **Pengoptimuman Corak:** Model LLM direka untuk meramalkan perkataan atau frasa seterusnya yang paling mungkin berdasarkan data yang dilihat. Kadangkala, corak statistik yang paling kuat mungkin bukan maklumat yang paling tepat dari segi fakta.

> **Kekurangan Konteks Masa Nyata (Grounding):** Model AI mungkin tidak mempunyai akses kepada maklumat terkini atau disahkan. Apabila diminta mengenai sesuatu di luar skop data latihannya, ia akan mengisi jurang dengan maklumat yang direka.

> **Kekaburan Pertanyaan (Ambiguity):** Pertanyaan yang tidak jelas atau terlalu terbuka boleh mendorong model untuk membuat andaian atau menggabungkan maklumat daripada pelbagai sumber secara tidak betul lalu menghasilkan output yang salah.

Kesan halusinasi boleh menjadi serius terutamanya dalam bidang kritikal. Dalam bidang perubatan, maklumat kesihatan yang direka boleh membawa kepada diagnosis yang salah. Dalam bidang perundangan, rujukan kepada kes undang-undang yang tidak wujud boleh menjejaskan kes mahkamah. Oleh itu, keupayaan AI untuk menjana maklumat palsu dengan keyakinan yang tinggi mewakili risiko bahaya dan kehilangan kepercayaan yang signifikan.







Mengurus Risiko: Strategi untuk Integriti dan Kebolehpercayaan

Untuk memanfaatkan potensi AI sambil mengurangkan risikonya, pendekatan dwistrategik adalah diperlukan dengan menumpukan pada kedua-dua input (data) dan output (model).

A. Memperkukuh Integriti Data:

Pembersihan dan Pengesahan Data (Data Cleansing and Validation): Mengimplementasikan proses yang ketat untuk mengenal pasti dan membetulkan kesilapan data sebelum latihan.

Penjejakan Sumber Asal Data (Provenance Tracking): Untuk memanfaatkan keupayaan AI secara optimum serta mengurangkan risiko penggunaannya, pendekatan dwistrategik yang merangkumi pengurusan input dan pemantauan output perlu diberi penekanan.

Audit Bias: Melakukan audit yang kerap untuk mengenal pasti dan mengurangkan berat sebelah dalam data yang boleh membawa kepada keputusan yang tidak adil.

B. Mengatasi Halusinasi AI:

Pemerolehan Penjanaan Ditingkatkan (RAG – Retrieval-Augmented Generation): Mengintegrasikan model AI dengan pangkalan data dan sumber maklumat yang dipercayai bagi menghasilkan respons yang lebih tepat, relevan dan berasaskan fakta yang disahkan.

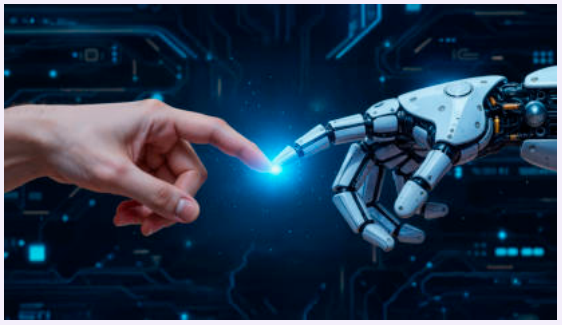
Kejuruteraan Prompt (Prompt Engineering): Mereka bentuk arahan yang jelas dan berstruktur bagi menghasilkan respons AI yang tepat, telus serta mengiktiraf ketidakpastian apabila maklumat tidak dapat disahkan.

Pengawasan Manusia (Human Oversight): Memastikan output AI disemak dan disahkan oleh pakar sebelum digunakan bagi menjamin ketepatan serta mengurangkan risiko maklumat yang tidak sahih.

Kesimpulan

Integriti data dan risiko halusinasi saling berkait dalam pembangunan AI. Bagi memastikan AI beroperasi secara tepat, bertanggungjawab dan dipercayai, standard integriti data yang tinggi perlu dipatuhi melalui pengurusan data yang sistematik serta langkah mitigasi seperti RAG dan pengawasan manusia. Pendekatan ini membantu meningkatkan kepercayaan terhadap AI dan memastikan manfaat yang berterusan kepada masyarakat.





BYTE BACK THE SCAMMERS

BIJAK DI DUNIA DIGITAL, SELAMAT SETIAP MASA



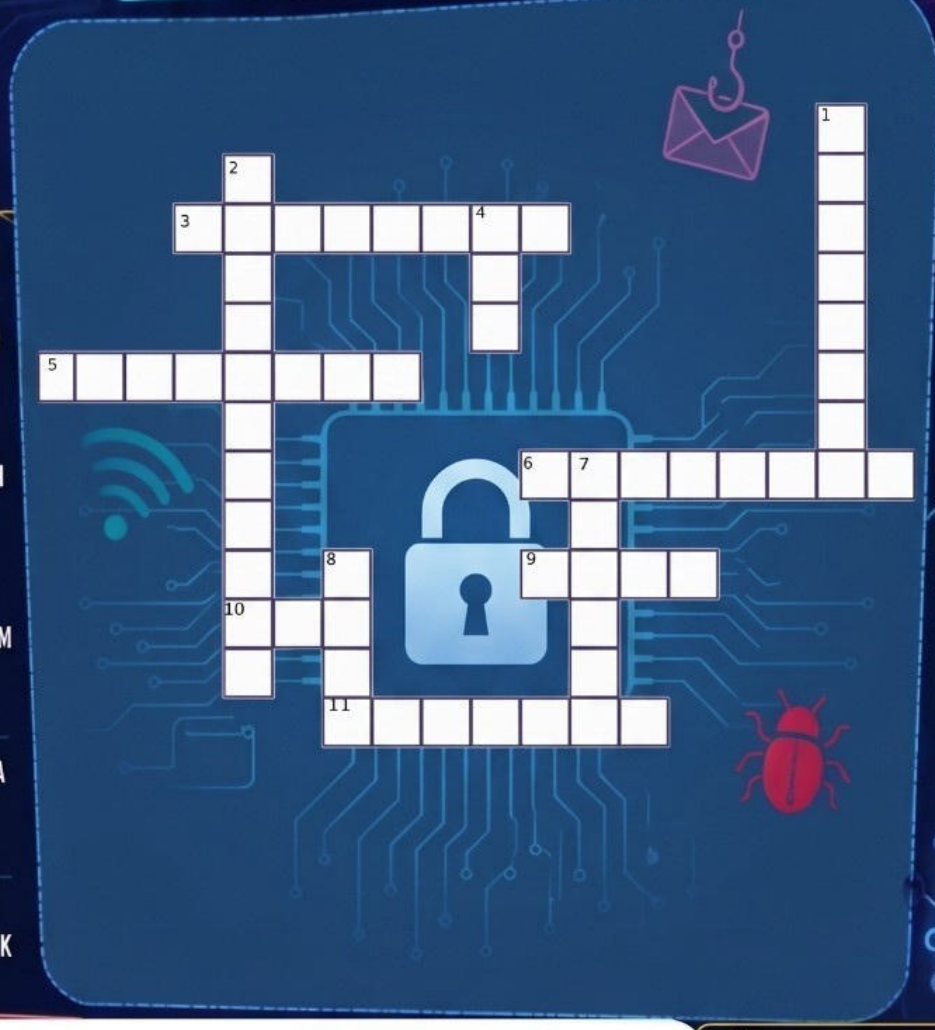
AWAS SCAMMER SENTIASA MENGINTAI!

FIKIR SEBELUM KLIK, ELAK JADI MANGSA!



INGAT!

- JANGAN KONGSI MAKLUMAT PERIBADI
- JANGAN MUDAH PERCAYA TAWARAN MENARIK
- SEMAK SEBELUM KLIK PADA PAUTAN
- GUNAKAN KATA LALUAN YANG KUAT & UNIK
- JIKA RAGU, HUBUNGI PIHAK YANG SAH



LINDUNGI DIRI ANDA, LINDUNGI DATA ANDA!



MENDATAR

3. Platform media sosial yang sering digunakan scammer.

5. Langkah keselamatan menggunakan kata laluan rahsia.

6. Aktiviti menghantar pautan palsu melalui emel atau mesej.

9. Unit polis yang berkaitan janayah siber di Malaysia.

10. Jangan kongsi nombor ini kepada orang lain.

11. Perisian berbahaya yang menyerang komputer.

MENEGAK

1. Tindakan memperdaya mangsa demi wang.

2. Laman web palsu yang menyerupai laman sebenar.

4. Kod keselamatan sekali guna.

7. Individu yang mencuri maklumat peribadi secara online.

8. Penipuan yang meminta TAC atau OTP bank.

JAWAPAN

SILA IMBAS QR CODE UNTUK JAWAPAN





JADILAH PENGGUNA DIGITAL YANG BIJAN!

BYTE BACK THE SCAMMERS!

#StayAlert #StaySafe #CyberSmart



WAR OF THE WORLD

MEDAN PERANG DIGITAL

ANTARA AMERIKA SYARIKAT DAN IRAN

Apabila algoritma, AI dan dron mengambil alih medan tempur, peperangan moden tidak lagi mengenal sempadan fizikal.

Oleh: Mohamed Amir Husaini bin Abdul Hamid

“Teknologi maklumat bukan lagi sekadar alat sokongan tetapi bertindak sebagai senjata utama.”

PEPERANGAN DIGITAL

Dunia kini bukan lagi sekadar berperang dengan peluru dan meriam di parit-parit tanah. Di bawah langit Timur Tengah yang membara pada tahun 2026, sebuah paradigma baharu telah muncul: Peperangan Digital. Ketegangan geopolitik antara Amerika Syarikat (AS) dan Iran telah beralih daripada pertembungan fizikal tradisional kepada perang pintar yang dipacu oleh algoritma, sistem navigasi satelit (GPS) dan rangkaian dron autonomi.

Artikel ini mengupas bagaimana teknologi digital menjadi tulang belakang konflik, statistik ekonomi yang mengejutkan serta impak mendalamnya terhadap ekosistem global.

AI + GPS + DRON

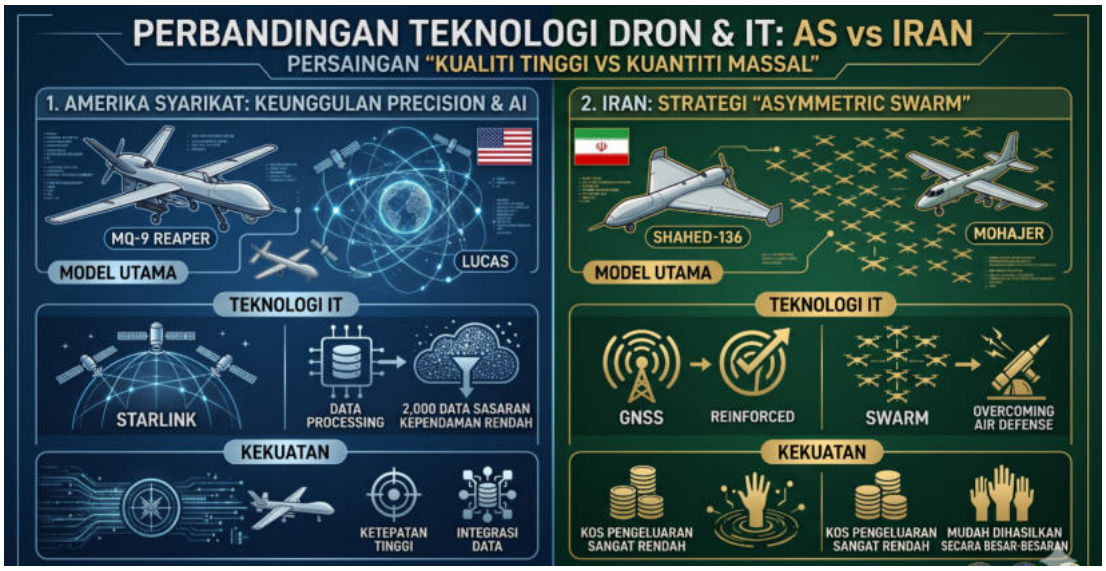
Tiga teknologi yang membentuk medan tempur digital moden.



SINERGI IT DALAM KETENTERAAN

DRON • GPS • AI

INFOGRAFIK



TEKNOLOGI SEBAGAI SENJATA

Dalam konflik terbaharu ini, teknologi maklumat bukan lagi sekadar alat sokongan tetapi bertindak sebagai senjata utama. Penggunaan Global Positioning System (GPS) dan Kecerdasan Buatan (AI) telah mengubah dron daripada sekadar pesawat pemantau menjadi pemusnah tepat.

1. Dron Autonomi: Kedua-dua pihak menggunakan dron yang dilengkapi AI untuk mengecam sasaran secara automatik tanpa penglibatan manusia sepenuhnya.

2. Peperangan Elektronik (EW): Fokus utama IT dalam perang ini adalah untuk membutakan musuh melalui gangguan isyarat GPS (GPS jamming) dan manipulasi data navigasi (spoofing).

3. Integrasi AI: AS telah memperkenalkan sistem LUCAS, sebuah ekosistem AI yang membolehkan segerombolan dron (swarming) berkomunikasi sesama sendiri untuk menyerang sasaran secara kolektif.

STATISTIK KOS PEPERANGAN

Walaupun dron sering dianggap murah, kos keseluruhan operasi melibatkan infrastruktur IT, satelit dan pertahanan siber adalah sangat besar.

PERKARA	AMERIKA SYARIKAT (US)	IRAN
Kos Operasi (Bulan Pertama)	~RM 12 Bilion (AS$2.5b+)	~RM 4.5 Bilion (AS$1b+)
Kos Purata Dron (Satu Unit)	AS30,000(LUCAS) -AS3 0j (Reaper)	AS20,000-AS50,000 (Shahed)
Kerugian Infrastruktur IT	Tinggi (Pangkalan Radar & Satelit)	Sangat Tinggi (Kemudahan Nuklear & Kilang Dron)
Jumlah Sasaran AI	13,000+ sasaran (Operasi Epic Fury)	Fokus pada pangkalan serantau & kapal

Nota: Pentagon dilaporkan membelanjakan hampir AS$6 bilion pada minggu pertama konflik untuk menggerakkan aset teknologi tinggi dan sistem pertahanan peluru berpandu.







FAKTA KONFLIK & KESAN GLOBAL

FAKTA-FAKTA TEPAT MENGENAI KONFLIK 2026

1. Operasi Epic Fury: AS melancarkan lebih 1,000 serangan dron menggunakan AI pada hari pertama untuk melumpuhkan pusat data dan komunikasi Iran.

2. Kemandirian Dron Iran: Walaupun diserang hebat, Iran berjaya mengekalkan 50% daripada program misil dan dronnya melalui pengeluaran bawah tanah yang tidak berpusat.

3. Kesan Orang Awam: Penggunaan AI dalam pemilihan sasaran masih mengundang kontroversi dengan laporan lebih 1,700 kematian orang awam akibat kesilapan algoritma atau data risikan yang tidak tepat.

"Kemenangan dalam perang moden hanyalah satu ilusi kerana kos kemanusiaan dan ekosistem adalah terlalu tinggi."



KESAN TERHADAP EKOSISTEM DUNIA

Peperangan berteraskan IT ini membawa impak yang melangkaui sempadan fizikal:

• Pencemaran Data & Siber: Serangan siber ke atas infrastruktur tenaga menyebabkan gangguan bekalan elektrik di beberapa negara jiran, menjejaskan hospital dan sistem air.

• Rantaian Bekalan Semikonduktor: Permintaan mendadak untuk cip AI bagi kegunaan perang menyebabkan krisis bekalan peranti elektronik global, meningkatkan harga komputer dan telefon pintar.

• Jejak Karbon Digital: Pusat data yang memproses simulasi perang dan algoritma AI menggunakan tenaga elektrik yang sangat tinggi dan menyumbang kepada peningkatan pelepasan karbon global.

• Ketidakstabilan GPS Global: Aktiviti jamming yang meluas di zon konflik mengganggu navigasi penerbangan awam dan perkapalan komersial di seluruh dunia serta meningkatkan risiko kemalangan.

EMPAT GELOMBANG IMPAK

- **Siber**
- **Semikonduktor**
- **Karbon digital**
- **Navigasi GPS**





KESIMPULAN

TEKNOLOGI TANPA ETIKA ADALAH RISIKO TAMADUN

"War of the World" dalam era digital ini membuktikan bahawa teknologi boleh menjadi agen pemusnah yang paling kejam dalam sejarah manusia jika tidak dikawal dengan etika. Walaupun teknologi IT menjanjikan serangan tepat, realitinya ia tetap membawa kemusnahan harta benda dan kehilangan nyawa yang tidak ternilai harganya.

Kita perlu menyedari bahawa kemenangan dalam perang moden hanyalah satu ilusi kerana kos kemanusiaan dan ekosistem adalah terlalu tinggi. Pemimpin dunia haruslah:

01

1. Memperkasakan Diplomasi Digital: Menggunakan platform IT untuk dialog, bukannya sebagai alat sabotaj.

02

2. Kawalan Etika AI: Menetapkan undang-undang antarabangsa yang melarang penggunaan AI sepenuhnya dalam membuat keputusan hidup atau mati tanpa pengawasan manusia.

03

3. Pelaburan dalam Keamanan: Mengalihkan bajet berbilion ringgit daripada teknologi senjata kepada teknologi hijau dan pendidikan.



Keamanan dunia bukanlah tanggungjawab teknologi tetapi tanggungjawab hati manusia yang mengendalikannya. Usah kita membiarkan algoritma menentukan masa depan tamadun kita.

UNIVERSITI SAINS MALAYSIA

TRANSFORMASI DIGITAL USM

MEMPERKASA WARGA AKADEMIK DAN PENGURUSAN PROFESIONAL DENGAN

GOOGLE GEMINI AI PRO



Disediakan oleh: Ts. Zaiyana Binti Mohamed Hussain

LATAR BELAKANG & MATLAMAT

Selaras dengan **Lonjakan 9 Pelan** Pembangunan Pendidikan Malaysia (Pendidikan Tinggi), Universiti Sains Malaysia (USM) kini mengorak langkah proaktif dengan menyediakan akses **Google Gemini AI Pro** kepada warga universiti **gred SSPA 9 dan ke atas** bermula **Mac 2026 sehingga Januari 2027** di semua kampus. Inisiatif ini direka untuk meningkatkan produktiviti, kreativiti dan kecekapan pengurusan data dalam ekosistem akademik yang kian mencabar.



TEMPOH KETERSEDIAAN LESEN

Pihak Kementerian Pengajian Tinggi melalui universiti telah menetapkan tempoh ketersediaan lesen seperti berikut:

Tarikh Mula:
1 Februari 2026

Tarikh Tamat:
31 Januari 2027

Status Semasa:
Sehingga kini, **30%** daripada pengguna terpilih telah mula mengaktifkan dan memanfaatkan fungsi AI ini dalam tugasan harian mereka.

MANFAAT UTAMA

Meningkatkan Produktiviti

Mempercepatkan penyediaan dokumen, analisis dan komunikasi harian.

Merangsang Kreativiti

Membantu penjanaan idea, visualisasi dan penyediaan bahan pembentangan yang lebih menarik.

Kecekapan Pengurusan Data

Memudahkan pemprosesan set data besar serta menghasilkan analisis dan visualisasi dengan lebih pantas.

APLIKASI DALAM EKOSISTEM USM

Penulisan & Penyuntingan Pintar

Merangka kertas kerja, emel profesional dan cadangan penyelidikan lebih cepat dengan menggunakan **Google Docs** dan **Gmail**.

Analisis Data Kompleks

Memproses set data besar dalam **Google Sheets** menggunakan arahan bahasa semula jadi untuk menghasilkan formula dan visualisasi.

NotebookLM untuk Rujukan

Membolehkan pengguna memuat naik dokumen rujukan dan berinteraksi dengan bahan tersebut untuk mendapatkan ringkasan atau jawapan fakta secara spesifik.

KESELAMATAN DATA

Data adalah terjamin kerana versi Pro memastikan data universiti tidak digunakan untuk melatih model AI awam sekaligus melindungi harta intelek warga USM.



APLIKASI DALAM TUGASAN HARIAN

Perkhidmatan	Kegunaan untuk Ahli Akademik & Pegawai
Google Docs	Menjana struktur syllabus, ringkasan minit mesyuarat dan membaiki gaya bahasa penulisan akademik.
Google Slides	Mencipta visual dan susun atur slaid pembentangan kuliah secara automatik berdasarkan teks.
Google Sheets	Automasi klasifikasi data pelajar atau analisis trend penyelidikan tanpa perlu menghafal formula rumit.

CARA LOG MASUK & PENGAKTIFAN AKAUN

Semua warga USM yang layak boleh mengakses perkhidmatan ini melalui portal rasmi Bahagian Tadbir Urus Digital. Sila ikuti langkah-langkah di bawah:

1. Layari pautan rasmi: https://digital.usm.my/servis/bahagian-tadbir-urus-digital/seksen-perkhidmatan-awan#google-workspace-for-education
2. Log masuk menggunakan **ID Identiti USM** anda.
3. Pastikan anda menggunakan akaun **Google Workspace** rasmi universiti **(@usm.edu.my)**.
4. Cari ikon **Gemini** (berbentuk bintang) pada bar sisi aplikasi **Google** anda untuk mula menggunakan fungsi AI Pro.

JOM AKTIFKAN SEKARANG!

USM menyeru baki **70%** pengguna yang belum mengaktifkan lesen ini untuk segera berbuat demikian bagi memastikan sumber digital universiti dimanfaatkan sepenuhnya.

> ***AI bukan untuk menggantikan kepakaran kita tetapi untuk membebaskan kita daripada tugasan rutin demi fokus kepada inovasi yang lebih bermakna.***

Kepercayaan Digital Terancam: Melawan Scam & Penipuan Siber

Taktik & Ancaman Penipuan Siber

Manipulasi Emosi & Kejuruteraan Sosial

Penipu menggunakan perasaan takut atau keinginan untung cepat untuk memperdaya mangsa memberikan akses maklumat.

Teknologi AI & Deepfake

Penggunaan AI untuk meniru suara dan wajah menjadikan penipuan kini jauh lebih sukar dikesan.

Phishing & Laman Web Palsu

Penggunaan pautan mencurigakan untuk mencuri maklumat sensitif dan wang mangsa melalui penyamaran identiti.



Dunia digital masa kini bergantung sepenuhnya kepada "kepercayaan digital", namun kepercayaan ini sedang diancam oleh taktik penipuan siber yang kreatif dan manipulatif. Daripada kajuruteraan sosial sehinggalah penggunaan teknologi AI, pengguna perlu memahami ancaman ini untuk mengambil langkah perlindungan yang tepat.

Langkah Mempertahankan Kepercayaan Digital



Pengesahan Dua Faktor (2FA)

Aktifkan 2FA dan gunakan kata laluan yang kuat untuk mengukuhkan keselamatan akaun anda.



Kawalan Maklumat Peribadi

Elakkan berkongsi maklumat peribadi secara sewenang-wenangnya dalam sebarang interaksi digital atau media sosial.



Sikap Waspada & Proaktif

Sentiasa berhati-hati sebelum kiik pautan dan laporkan sebarang aktiviti mencurigakan kepada pihak berkuasa.

Disediakan oleh:
Jamaliah Shafiei

Mereka Tidak Menggodam Sistem, Mereka Menggodam Manusia

Scammer moden tidak lagisekada rmemecah masuk kod komputer, sebaliknya mereka mengeksploitasi kelemahan manusia seperti emosi dan kepercayaan. Melalui tiga kajian kes dokumentari popular, kita dapat melihat bagaimana teknologi hanyalah alat untuk memanipulasi mangsa secara psikologi.

Tiga Kisah Benar Popular yang menarik perhatian dunia



The Tinder Swindler : Manipulasi Emosi

"Satu *swipe* membawa kepada perkenalan, satu mesej membawa kepada kepercayaan dan satu pautan transaksi membawa kepada kehancuran."



Inventing Anna : Identiti Digital Palsu

Identiti digitalbolehdirekadengan gayahidup mewahdi media sosial untuk membina kredibiliti dan pengaruh yang tidak wujud.



The Great Hack : Data Sebagai Senjata

Mengumpuljejakdigital(likes/komen)untuk membinaprofil dan mempengaruhi tingkah laku manusia secara halus.

Byte Back the Scammers



Manusia Adalah Sasaran Sebenar

Scammer mungkin mempunyai teknologi yang semakin maju tetapi mereka hanya akan berjaya apabila manusia gagal berfikir secara kritikal.



Stop, Check & Verify

Sebelum mempercayai sesuatu yang dilihat di skrin, kita perlu berhenti seketika untuk berfikir, menyemak dan mengesahkan.



Celik Digital

Membina masyarakat yang lebih celik digital, berfikiran kritikal dan mampu membezakan antara realiti dan manipulasi.

Disediakan oleh: Nurzalina Nordin

Klik, Percaya, Lesap: Kenali Taktik Scammer & Cara Lindungi Diri

FASA PENIPUAN: BAGAIMANA WANG ANDA LESAP

KLIK: Jerat Phishing & Spoofing



Scammer menghantar pautan palsu (SMS/e-mel) untuk mencuri butiran peribadi dan kata laluan bank.

Taktik:	Mekanisme:	Impak:
Phishing	Laman web tiruan (*cloned*)	Pencurian dana serta-merta

PERCAYA: Skim Pelaburan & Kerja Palsu



Menawarkan pulangan tinggi atau gaji lumayan untuk membina kepercayaan sebelum melarikan pelaburan mangsa.

Taktik:	Mekanisme:	Impak:
Skim Kerja	Testimonial palsu	Kehilangan modal besar

KETAKUTAN: Panggilan Berkuasa & Malware



Menyamar sebagai polis/bank untuk mendesak mangsa memuat turun aplikasi "siasatan" yang sebenamya mencuri data.

Taktik:	Mekanisme:	Impak:
Malware	Aplikasi tidak rasmi	Pindahan wang tanpa izin

TIGA GARIS PERTAHANAN UTAMA



Semak Sebelum Klik

Pastikan URL adalah sah dan hubungi institusi melalui nombor rasmi, bukan nombor penghantar mesej.



Rahsiakan Maklumat Sensitif

Institusi sah tidak akan meminta OTP, TAC atau kata laluan melalui panggilan atau mesej.



Aktifkan Benteng Digital

Gunakan pengesahan dua faktor (2FA) dan kemaskini perisian antivirus secara berkala.

Disediakan oleh:
Sharifah Shakila MD Saad

Memperkasa Pertahanan Siber:

Bagaimana USM Menguasai Piawaian Keselamatan Maklumat Bertaraf Dunia

Dari data akademik hingga kerjasama universiti, USM membina pertahanan digital berdaya tahan melalui piawaian keselamatan maklumat antarabangsa.

OLEH MAHADI YUSOF



Pengenalan: Data Institusi, Aset Paling Berharga

Di tengah gelombang transformasi digital yang melanda sektor pendidikan, maklumat telah menjadi aset paling strategik. Bagi Universiti Sains Malaysia (USM), sebuah institusi penyelidikan awam yang terkemuka, melindungi data sensitif yang merangkumi rekod akademik pelajar, penyelidikan proprietari dan maklumat peribadi staf adalah keutamaan mutlak.

Komitmen ini diterjemahkan melalui implementasi Sistem Pengurusan Keselamatan Maklumat (ISMS) yang teguh dan berpandukan standard antarabangsa yang paling diiktiraf: ISO/IEC 27001.

> **“Di tengah gelombang transformasi digital yang melanda sektor pendidikan, maklumat telah menjadi aset paling strategik.”**

Transisi Strategik ke ISO/IEC 27001:2022

USM telah mengambil langkah proaktif dengan menaik taraf pensijilan kepada versi terkini, iaitu ISO/IEC 27001:2022. Versi terbaharu ini bukan sekadar kemaskini kosmetik tetapi ia adalah rangka kerja komprehensif yang diperkemas untuk menangani landskap ancaman siber yang semakin canggih.

Versi 2022 memberikan penekanan yang lebih mendalam terhadap aspek Keselamatan Siber (Cybersecurity) dan Perlindungan Privasi (Privacy Protection).

ISMS bukanlah sekadar sijil di dinding tetapi merupakan rangka kerja sistematik yang menjamin tiga tonggak utama keselamatan maklumat:

• Kerahsiaan (Confidentiality): Data hanya boleh diakses oleh pihak yang sah.

• Integriti (Integrity): Data kekal tepat, lengkap dan tidak diubah tanpa kebenaran.

• Ketersediaan (Availability): Sistem dan maklumat sentiasa sedia untuk digunakan.

Melalui inisiatif ini, USM memberikan jaminan kepada seluruh warga universiti dan pihak berkepentingan bahawa infrastruktur ICT mereka selamat dan terkawal.

Melindungi jantung digital universiti

Skop Operasi: Melindungi Jantung Digital USM

Pensijilan ISMS USM difokuskan secara strategik pada sistem yang menjadi nadi operasi harian universiti:

Sistem Maklumat Universiti - Pelajar (SMU-P): Menguruskan data penting akademik dan peribadi seluruh komuniti pelajar.

Sistem Maklumat Universiti - Staf (SMU-S): Mengendalikan data berkaitan pentadbiran dan perkhidmatan kakitangan.

Kedua-dua sistem kritikal ini beroperasi di Kampus Induk dan diuruskan oleh Pusat Transformasi Digital (PTD) yang dahulunya dikenali sebagai Pusat Pengetahuan, Komunikasi & Teknologi (PPKT). USM memilih untuk mengecualikan sistem kewangan dan klinikal (SMU-Kewangan dan SMU-Klinikal) dalam fasa pensijilan semasa bagi memastikan fokus perlindungan adalah padu dan optimum.

SIDEBAR / RINGKASAN ARTIKEL

Tiga tonggak ISMS

1. Kerahsiaan (Confidentiality): Data hanya boleh diakses oleh pihak yang sah.
2. Integriti (Integrity): Data kekal tepat, lengkap dan tidak diubah tanpa kebenaran.
3. Ketersediaan (Availability): Sistem dan maklumat sentiasa sedia untuk digunakan.

Garis Masa Kejayaan: Maraton Keselamatan yang Berterusan

Perjalanan USM dalam ISMS adalah bukti komitmen jangka panjang dengan SIRIM QAS International bertindak sebagai badan pensijilan:

- **2015–2018 (Asas Kukuh):**

  Inisiatif bermula pada 2015 dan kemuncaknya USM memperoleh pensijilan pertamanya pada 25 Mei 2018.

- **2019–2021 (Kekal Relevan):**

  USM berjaya mengekalkan pematuhan dengan audit tahunan dan dianugerahkan pensijilan baharu pada 8 Jun 2021.

- **2022–2024 (Lompatan Strategik):**

  Kitaran terkini menyaksikan transisi kritikal kepada piawaian ISO/IEC 27001:2022 yang memberi tumpuan kepada Keselamatan Siber. Selepas Audit Pensijilan Semula pada Mei 2024, USM sekali lagi dianugerahkan pensijilan baharu pada 7 Jun 2024 dan sah sehingga Mei 2027.



CERTIFIED TO ISO/IEC 27001:2022
CERT. NO. : ISMS 000314



CERTIFIED TO ISO/IEC 27001:2022
CERT. NO. : ISMS 000314



CERTIFIED TO ISO/IEC 27001:2022
CERT. NO. : ISMS 000314

> **“Ini membuktikan bahawa keselamatan siber adalah tanggungjawab kolektif bukan hanya pasukan IT.”**

Keselamatan ialah tanggungjawab bersama

Ekosistem ISMS: Keselamatan sebagai Tanggungjawab Kolektif

Kejayaan implementasi ini adalah hasil daripada penglibatan strategik dan kerjasama seluruh jabatan. Ini membuktikan bahawa keselamatan siber adalah tanggungjawab kolektif bukan hanya pasukan IT.

Entiti Utama	Peranan Kritikal dalam ISMS
PTD / PPKT	Pengurusan teknikal, pemantauan sistem maklumat dan pelaksanaan kawalan.
Jabatan Pembangunan & Pengurusan Fasiliti	Penyelenggaraan kritikal peralatan elektrik dan infrastruktur pusat data.
Jabatan Pendaftar	Pengurusan tapisan staf bagi memastikan kerahsiaan maklumat peribadi.
Pejabat Perundangan Universiti	Mengendalikan kontrak dan Perjanjian Kerahsiaan (NDA) berkaitan maklumat sensitif.
Jabatan Bendahari	Penilaian pembekal dan pihak ketiga dari sudut pematuhan keselamatan maklumat.

Inovasi Kolaboratif: Mengangkat Standard Keselamatan Negara

Satu ciri unik dalam ekosistem ISMS USM ialah inisiatif perkongsian kepakaran dengan rakan Universiti Awam (UA) lain seperti UTHM, UNIMAS, UNIMAP, UMPSA, UMT dan USIM.

Wakil-wakil dari UA ini diundang sebagai juruaudit dan pemerhati dalam Audit Dalaman ISMS USM. Langkah berani ini berfungsi sebagai platform untuk pertukaran kepakaran, pendedahan kepada kaedah pengauditan silang yang terbaik dan secara tidak langsung membantu mengangkat piawaian keselamatan siber di peringkat kebangsaan.

> **“USM telah menetapkan penanda aras baharu bagi keselamatan digital dalam institusi pengajian tinggi awam.”**

Kesimpulan: USM Peneraju Berdaya Tahan Digital

Pensijilan ISO/IEC 27001:2022 yang berterusan, disokong oleh komitmen yang tersusun dan ekosistem yang kohesif, membuktikan bahawa USM bukan sahaja cemerlang dalam bidang akademik tetapi juga merupakan model kepimpinan dalam pengurusan infrastruktur maklumat yang patuh dan berdaya tahan terhadap ancaman siber masa kini. USM telah menetapkan penanda aras baharu bagi keselamatan digital dalam institusi pengajian tinggi awam.

DISEDIAKAN:

MAHADI YUSOF

Ketua Bahagian

Bahagian Tadbir Urus Digital

Pusat Transformasi Digital, USM



Pernah tak rasa nak buang laptop bila keluar "Wrong Password"?
Bila tukar password baharu, keluar pula "New password cannot be the same as old password"!!!
Jangan pening kepala! Sebelum laptop jadi mangsa, hubungi Team Servisdesk di EXT 5333.
Biar kami bantu selesaikan masalah log masuk anda.

Disediakan oleh: Shariza Shaari

Siapa Sebenarnya *Scammer*???

REAL-LOOKING # REAL

SIASATAN KESEDARAN SIBER



Digital kini, kita banyak membincangkan isu penipuan dalam talian lazimnya berkaitan penjual yang tidak jujur. Mereka berjanji untuk menghantar produk berkualiti sebaliknya menghantar barang yang salah atau lebih teruk lagi, menghilangkan diri selepas menerima bayaran. Sehingga kita menyedari perkara tersebut dan sentiasa berwaspada hasil daripada pengalaman diperdaya dan ditipu sebelum ini.

Namun, bagaimana sekiranya penjenayan siber (scammer) ini bukanlah di pihak yang menjual, tetapi di pihak yang membeli? Seterusnya, bagaimana jika scammer ini yang menjalankan aktiviti rutin secara berulang tanpa menyedari dirinya adalah punca kerugian dan kesusahan kepada mangsa?

Perkenalkan Suparjo (bukan nama sebenar), seorang pembeli dalam talian yang aktif dan sentiasa bangga dengan gelaran sebagai “pengguna bijak”. Suparjo membeli dari pelbagai kedai kecil terutamanya perniagaan buatan tangan (home-based) yang diuruskan oleh suri rumah atau pelajar. Dia tiada sebarang niat tetapi dia percaya haknya sebagai pembeli memberikannya kuasa mutlak seperti mana kata-kata “customer is always right”.

Tindakan ‘scamming’ Suparjo bermula dari tuntutan yang nampak remeh tetapi memberi ingat kepada perniagaan kecil secara perlahan.

Tawar-Menawar Ekstrem:

Suparjo akan menawar harga barang hingga ke paras yang sangat tidak munasabah, seringkali di bawah kos bahan mentah dan upah penjual. Jika penjual menolak, Suparjo akan menggunakan taktik emosi, mengatakan dia adalah pelanggan yang setia atau hanya ‘mampu’ pada harga itu. Penjual kecil takut kehilangan jualan dan bimbang akan ulasan negatif, selalunya terpaksa mengalah dan menerima keuntungan yang hampir sifar atau lebih teruk mengalami kerugian.

Permintaan Berlebihan dan Perubahan Minit Akhir

Untuk setiap pembelian, Suparjo sering meminta pembatalan percuma seperti pembungkusan hadiah yang rumi, penghantaran segera tanpa bayaran tambahan atau penyesuaian produk yang memakan masa berjam-jam. Selepas penjual menghabiskan masa dan tenaga memenuhi permintaan ini, Suparjo akan membatalkan pesanan pada saat-saat akhir kerana 'tiba-tiba tak jadi' atau menukar spesifikasi secara drastik sehingga produk asal tidak dapat dijual kepada orang lain.

Memulangkan barang yang telah diterima

Suparjo akan memulangkan barang yang diterima sekiranya tidak menarik minat walaupun telah digunakan memandangkan tempoh pemulangan secara percuma masih belum tamat. Lebih menyedihkan lagi apabila barang yang dipulangkan itu rosak atas kecuaian sendiri tetapi menggunakan alasan alat yang diterima rosak dan ada juga barang yang dipulangkan adalah bukan barang sebenar tetapi aplikasi talian telah membayar pampasan mengakibatkan kerugian ditanggung oleh penjual.

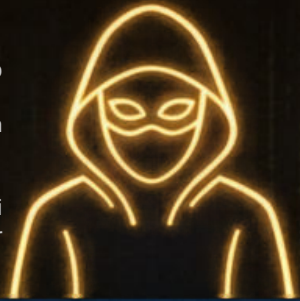
Acaman Ulasan Negatif

Ini adalah senjata utama Suparjo. Jika penjual enggan memenuhi permintaannya yang tidak munasabah, Suparjo akan mengugut untuk meninggalkan ulasan satu bintang yang menjejaskan reputasi kedai. Dalam dunia perniagaan atas talian yang bergantung pada rating, ancaman ini cukup untuk memaksa penjual menyerah, memberikan barangan percuma atau memulangkan wang walaupun tiada kesalahan dilakukan oleh mereka.

Suparjo sentiasa menganggap tindakan ini sebagai 'berunding' atau 'menjaga kepentingan diri'. Baginya, dia hanyalah seorang pengguna yang menuntut perkhidmatan yang terbaik. Dia tidak pernah melihat wajah putus asa di sebalik skrin penjual atau mengira kerugian kewangan yang ditanggung oleh individu yang bergantung pada perniagaan kecil itu untuk menyara keluarga.

Dia tidak pernah sedar bahawa setiap 'kemenangan' tawar-menawarnya, setiap pembatalan pesanan yang santai dan setiap ancaman ulasan buruk telah melucutkan rezeki orang lain, mencuri masa, tena
ga dan harapan mereka. Suparjo, tanpa sebarang kesedaran telah menjadi penipu ekonomi dan seorang yang menggunakan kuasa pembeli untuk memanipulasi dan memeras ugut peniaga kecil sehingga ke tahap kerugian.

Dalam kes ini, Suparjo tidak pernah sedar kezaliman yang dilakukannya. Dia terus beroperasi dengan pemikiran sebagai 'pembeli bijak', tidak pernah menyedari bahawa di mata penjual yang telah menjadi mangsa manipulasinya, dia adalah scammer paling berbahaya yang tidak memakai topeng scammer tetapi memakai topeng pengguna.



OLEH: SHEIKH MD ROSHAHIDI BIN SHEIKH DAUD

SIAPA SEBENARNYA DI SEBALIK SKRIN?

Scammer di IPT



Sindiket penipuan (*scammer*) dalam rangkaian universiti merujuk kepada taktik licik penjenayah siber yang menyasarkan mahasiswa, pensyarah dan kakitangan institusi pengajian tinggi (IPT). Walaupun warga universiti dianggap celik teknologi, pihak polis dan pentadbiran IPTA/IPTS kerap mengeluarkan amaran kerana kes penipuan yang melibatkan kerugian ratusan ribu ringgit terus meningkat.

Berikut adalah modus operandi utama yang sering dikesan dalam ekosistem universiti:

1 Penipuan Emel Siswa Palsu & Pembayaran Yuran



Taktik: Scammer menghantar emel atau mesej WhatsApp yang menyerupai saluran rasmi universiti. Mereka mendakwa akaun pelajar akan disekat sekiranya tidak membayar yuran pengajian dengan segera ke akaun bank peribadi atau pihak ketiga yang diberikan.

Contoh Insiden:
Kesatuan Mahasiswa Universiti Malaya (KMUM) dan Universiti Kuala Lumpur (UniKL) pernah mengeluarkan amaran keras mengenai taktik emel palsu ini.

2 Tawaran Biasiswa & Bantuan Kewangan Palsu



Taktik:
Pelajar (terutamanya golongan B40 atau pelajar tahun satu) dihubungi melalui Telegram/WhatsApp dan ditawarkan biasiswa atau tajaan pendidikan yang lumayan. Namun, mangsa diwajibkan membayar "wang pendahuluan" atau "yuran pemprosesan" (sekitar RM200–RM500) sebelum dana dipindahkan ke akaun pelajar. Selepas bayaran dibuat, scammer akan menghilangkan diri.

3 Penipuan Sewa Rumah dan Bilik (Scam Rumah Sewa)



Taktik:
Menyasar pelajar senior atau pelajar luar kampus. Scammer mengiklankan bilik atau rumah sewa yang cantik dengan harga murah di media sosial. Pelajar diminta membayar wang cengkeram (deposit) dengan cepat kononnya kerana "permintaan tinggi" tetapi rumah tersebut sebenarnya tidak wujud.

4 Panggilan Palsu (Phone Scam / Courier Scam)



Taktik:
Mangsa menerima panggilan daripada individu yang menyamar sebagai pihak berkuasa (LHDN, mahkamah, polis atau syarikat kurier). Mereka menakut-nakutkan pelajar dengan mendakwa akaun mereka terlibat dalam aktiviti jenayah (seperti pengubahan wang haram atau penyeludupan barang). Akibat panik, ada pelajar yang sanggup memindahkan wang simpanan atau duit pinjaman pendidikan mereka.

5 Penipuan Pekerjaan Sambilan & Pelaburan Tidak Wujud



Taktik:
Mengambil kesempatan atas kesempitan wang pelajar dengan menawarkan kerja sambilan mudah dari rumah (e-commerce task) atau skim pelaburan berpulangan tinggi melalui platform dalam talian yang tidak sah.

Cara mengelak dan melindungi diri:

1 Sahkan Saluran Pembayaran

Universiti tidak pernah meminta bayaran yuran ke akaun peribadi individu atau melalui WhatsApp. Sentiasa gunakan portal kewangan rasmi universiti (seperti Portal MAYA untuk UM atau gerbang pembayaran rasmi yang ditetapkan).

2 Semak Domain Emel

Pastikan emel yang diterima menggunakan domain rasmi institusi (contohnya berakhir dengan @usm.my, @upm.edu.my, dll.)

3 Jangan Kongsi Maklumat Peribadi

Jangan sesekali menyerahkan nombor kad pengenalan, kata laluan perbankan atau kod OTP kepada sesiapa.

4 Gunakan Portal Semak Mule

Sebelum membuat sebarang transaksi ke akaun tidak dikenali, lakukan semakan nombor akaun bank atau nombor telefon di Portal Semak Mule PDRM.

JIKA ANDA ATAU RAKAN UNIVERSITI TELAH MENJADI MANGSA PENIPUAN KEWANGAN,
SEGERA HUBUNGI PUSAT RESPON PENIPUAN KEBANGSAAN (NSRC)
DI TALIAN 997 DALAM TEMPOH 24 JAM UNTUK MENYEKAT PENGALIRAN KELUAR WANG TERSEBUT.

OLEH: MOHAMAD KHAIRI BIN OSMAN

Lindungi Diri & Data: Panduan Menghadapi Ancaman Siber dan Penipuan (Scam)

Kenali Jenis Penipuan (Scam) Popular



Phishing (Pancingan Data)
Penipuan melalui emel atau mesej yang menyerupai sumber sah (bank/kerajaan) untuk mencuri maklumat log masuk dan kata laluan.



Penipuan Cinta (Love Scams) & Pelaburan
Taktik menyamar sebagai pasangan romantik atau menawarkan pulangan pelaburan tinggi yang tidak munasabah untuk memujuk mangsa memindahkan wang.



Taktik "Evil Twin" WiFi
Scammer membina hotspot WiFi palsu dengan nama yang hampir sama dengan tempat awam (cth: Lapangan Terbang (ABC) untuk mengintip aktiviti mangsa.

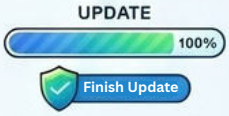
Langkah Keselamatan Peranti & Data



Gunakan Kata Laluan Kuat & Unik
Gabungkan huruf besar, huruf kecil, nombor dan simbol elakkan menggunakan maklumat peribadi yang mudah diteka seperti tarikh lahir.

Aktifkan Pengesahan Dua Faktor (2FA)
Tambah lapisan keselamatan biometrik atau PIN untuk memastikan hanya anda yang boleh mengakses akaun penting.





Kemas Kini Perisian (Updates) Secara Berkala
Kemas kini sistem operasi dan aplikasi mengandungi "patuh" keselamatan untuk menutup lubang yang boleh dieksploitasi penggodam.



Gunakan VPN (Virtual Private Network)
VPN menyulitkan (encrypt) data anda, menjadikannya sukar dipintas oleh pihak ketiga, terutama ketika menggunakan rangkaian yang kurang selamat.



Lindungi WiFi Rumah Anda



Ujian Manual "Pencuri WiFi"
Matikan semua peranti pintar di rumah; jika lampu modem masih berkelip laju, itu tandanya ada orang lain sedang menceroboh rangkaian anda.



Sembunyikan Nama WiFi (SSID)
Dengan menyembunyikan SSID, rangkaian anda tidak akan muncul dalam senarai carian automatik peranti orang luar.



Nyahaktifkan Fungsi WPS & UPnP
Ciri ini memudahkan sambungan tetapi mempunyai kelemahan keselamatan yang sering digunakan penggodam untuk menceroboh masuk.

Tip Keselamatan WiFi Awam



Elakkan Transaksi Perbankan
Jangan sekali-kali log masuk ke akaun bank atau e-dompet ketika menggunakan WiFi percuma di tempat awam.



Gunakan Data Mudah Alih Sendiri
Adalah lebih selamat untuk menggunakan pelan data telefon atau "roaming" berbanding menyambung ke WiFi awam yang tidak diketahui kesahihannya.



Sahkan Nama WiFi dengan Staf
Sentiasa tanya staf premis tentang nama rasmi WiFi mereka untuk mengelak daripada tersambung ke "hotspot" palsu milik hacker.

Tindakan Jika Menjadi Mangsa



Hubungi Talian 997 (NSRC)
Segera hubungi Pusat Respons Scam Kebangsaan (NSRC) jika anda menyedari wang telah dipindahkan keluar secara tidak sah.



Semak Melalui Portal "Semak Mule"
Gunakan portal rasmi PDRM (semakmule.rmp.gov.my) untuk memeriksa sama ada nombor akaun atau numbor telefon mempunyai rekod penipuan.



Laporkan kepada Bank & Pihak Berkuasa
Buat laporan polis dan maklumkan kepada pihak bank untuk menyekat akses akaun serta-merta bagi mengurangkan kerugian.

OLEH:
HISHAMMUDIN ENDAN

Oleh: Suhaimi Saibon

BitLocker: Pelindung Data atau Punca Masalah?

BitLocker melindungi data anda tetapi tanpa pengurusan Recovery Key yang betul, keselamatan boleh bertukar menjadi cabaran besar.

Dalam dunia digital hari ini, keselamatan data menjadi perkara yang sangat penting sama ada bagi individu mahupun organisasi. Banyak maklumat penting seperti dokumen rasmi, data pelanggan dan fail kerja disimpan di dalam komputer. Bagi membantu melindungi maklumat tersebut, sistem operasi Microsoft Windows menyediakan satu ciri keselamatan yang dikenali sebagai BitLocker.

BitLocker merupakan teknologi penyulitan cakera keras yang berfungsi untuk melindungi data daripada diakses oleh pihak yang tidak bertanggungjawab. Ciri ini biasanya terdapat pada komputer yang menggunakan Windows 10 dan Windows 11. Walaupun BitLocker mampu meningkatkan tahap keselamatan data namun terdapat beberapa cabaran yang sering dihadapi oleh pengguna.





Apa Itu BitLocker?

BitLocker ialah sistem keselamatan yang menyulitkan (encrypt) keseluruhan cakera keras komputer. Ini bermaksud semua data yang tersimpan dalam komputer dilindungi dengan sistem penyulitan khas.

Sekiranya komputer hilang atau dicuri, pihak lain tidak akan dapat membuka data tanpa Recovery Key iaitu kunci keselamatan khas yang digunakan untuk membuka cakera yang dilindungi.

“Jika pengguna kehilangan Recovery Key, data mungkin tidak dapat diakses semula.”

Kebaikan BitLocker

1. Melindungi Data Sensitif

BitLocker memastikan data penting seperti dokumen kerja dan maklumat peribadi tidak mudah diakses oleh pihak luar.

2. Keselamatan Tambahan Jika Komputer Hilang

Sekiranya komputer riba hilang atau dicuri, data di dalam cakera keras masih dilindungi oleh sistem penyulitan.

3. Integrasi Terus Dengan Windows

BitLocker dibangunkan oleh Microsoft, menjadikannya mudah digunakan tanpa perlu memasang perisian tambahan.

4. Sesuai Untuk Penggunaan Organisasi

Dalam persekitaran pejabat, BitLocker membantu melindungi data penting organisasi daripada risiko kebocoran maklumat.

Kelemahan BitLocker

1. Risiko Kehilangan Data

Jika pengguna kehilangan Recovery Key, data mungkin tidak dapat diakses semula.

2. Komputer Boleh Terkunci Secara Tiba-tiba

Kadangkala sistem akan meminta Recovery Key apabila berlaku perubahan seperti kemaskini BIOS atau perubahan perkakasan.

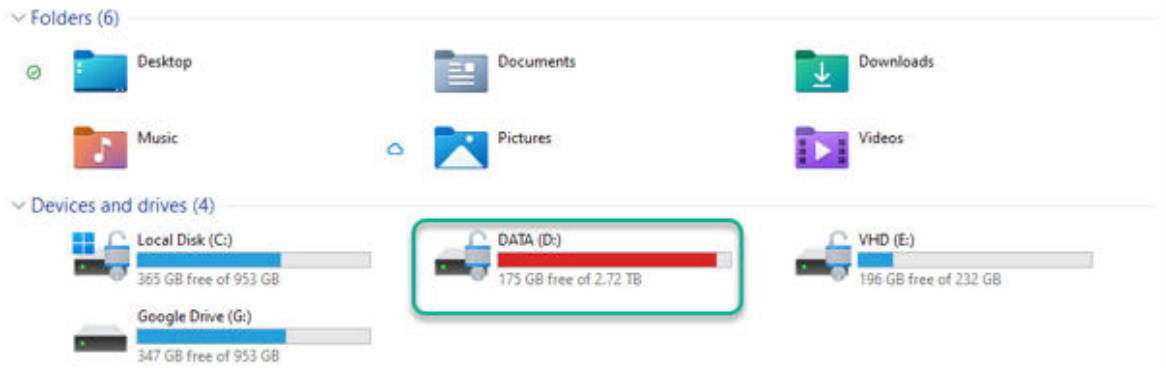
3. Menyukarkan Kerja Penyelenggaraan

Bagi juruteknik komputer, BitLocker boleh menyukarkan proses seperti format komputer, cloning cakera keras atau pemulihan data.

4. Sedikit Kesan Terhadap Prestasi

Walaupun tidak ketara pada komputer moden, proses penyulitan boleh memberi sedikit kesan kepada prestasi komputer lama.

“Ramai pengguna tidak menyedari perkara ini sehingga komputer mereka meminta Recovery Key secara tiba-tiba.”



Paparan1: Simbol kunci menunjukkan Bitlocker telah diaktifkan kepada ‘drives’

Tips & Amalan Terbaik

- Simpan Recovery Key di tempat yang selamat
- Buat backup data penting secara berkala
- Simpan Recovery Key dalam akaun Microsoft atau pemacu USB
- Berhati-hati ketika melakukan perubahan perkakasan

Tip Juruteknik IT

Sebelum melakukan kerja penyelenggaraan komputer seperti:

- Format semula sistem operasi
- Clone atau tukar SSD / HDD
- Kemaskini BIOS
- Tukar motherboard atau RAM

Pastikan BitLocker dimatikan terlebih dahulu atau Recovery Key disimpan dengan selamat.

Ini kerana sistem mungkin akan mengesan perubahan keselamatan dan meminta Recovery Key semasa komputer dihidupkan semula.

KENALI PAPARAN PEMULIHAN



Paparan 2: Paparan mesej yang meminta Recovery Key

Tahukah Anda?

Sesetengah komputer yang menggunakan Windows 11, BitLocker boleh aktif secara automatik jika peranti mempunyai cip keselamatan Trusted Platform Module (TPM).

Ramai pengguna tidak menyedari perkara ini sehingga komputer mereka meminta Recovery Key secara tiba-tiba.

“Dengan pengurusan yang baik, BitLocker boleh menjadi pelindung data yang berkesan bukan punca masalah kepada pengguna.”

Kesimpulan

BitLocker merupakan satu ciri keselamatan yang sangat berguna untuk melindungi data daripada akses tanpa kebenaran. Namun begitu, pengguna perlu memahami cara penggunaannya dengan betul dan memastikan Recovery Key disimpan dengan selamat.

Dengan pengurusan yang baik, BitLocker boleh menjadi pelindung data yang berkesan bukan punca masalah kepada pengguna.

FLASH FILL DI EXCEL

Simple Shaz

Isi Data Secara Pantas, Jimat Masa & Mudah!

Oleh : Shariza Sharuddin

CARA MENGGUNAKAN FLASH FILL

1 Sediakan Data:

Pastikan data yang ingin diubah (contoh: Nama Penuh) berada di sebelah kiri lajur kosong yang anda ingin letakkan hasil baharu (contoh: Nama Pertama).

	A	B
	Nama Penuh	Nama Pertama
1	Ahmad Bin Ali	
2	Siti Nur Aisyah	
3	Mohd Firdaus Rahman	
4	Nurul Syuhada Binti Zainal	
5	Lim Wei Sheng	

2 Taip Contoh (Pola):

Dalam sel pertama lajur kosong, taipkan hasil yang anda mahukan (contoh: taip nama pertama daripada nama penuh).

	A	B
	Nama Penuh	Nama Pertama
1	Ahmad Bin Ali	Ahmad
2	Siti Nur Aisyah	
3	Mohd Firdaus Rahman	
4	Nurul Syuhada Binti Zainal	
5	Lim Wei Sheng	

3 Aktifkan Flash Fill:

Kaedah 1 (Pantas): Tekan **Ctrl + E** pada papan kekunci anda.

Kaedah 2 (Ribbon): Pergi ke tab **Data** dan klik **Flash Fill** dalam kumpulan Data Tools.

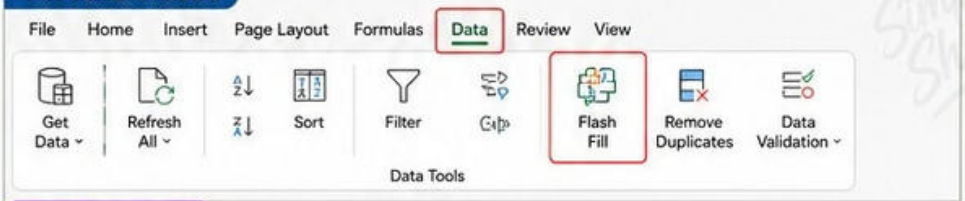
Kaedah 3 (Drag): Seret fill handle (penjuru kanan bawah sel) ke bawah, kemudian klik ikon Auto Fill Options dan pilih Flash Fill.

Kaedah 1: Pantas (Ctrl + E)

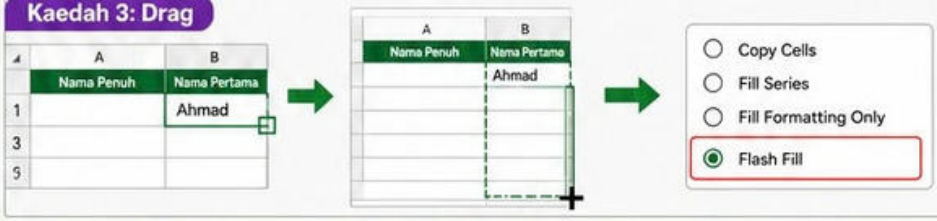


	A	B
	Nama Penuh	Nama Pertama
1	Ahmad Bin Ali	Ahmad
2	Siti Nur Aisyah	Siti
3	Mohd Firdaus Rahman	Mohd
4	Nurul Syuhada Binti Zainal	Nurul
5	Lim Wei Sheng	Lim

Kaedah 2: Ribbon



Kaedah 3: Drag



KEGUNAAN UTAMA FLASH FILL

Memisahkan Data

Mengambil nama depan daripada nama penuh.

Nama Penuh	Nama Pertama
Ahmad Bin Ali	Ahmad
Siti Nur Aisyah	Siti
Mohd Firdaus Rahman	Mohd

Menggabungkan Data

Menyatukan nama pertama dan nama akhir menjadi nama penuh.

Nama Pertama	Nama Akhir	Nama Penuh
Ahmad	Ali	Ahmad Ali
Siti Nur	Aisyah	Siti Nur Aisyah
Lim	Wei Sheng	Lim Wei Sheng

Menformat Data

Mengubah format tarikh atau menambah kod kawasan pada nombor telefon.

Data Asal	Hasil Baharu
01/05/2024	1 Mei 2024
15/08/2024	15 Ogos 2024
03/12/2024	3 Dis 2024

Data Asal	Hasil Baharu
012-345 6789	+60 12-345 6789
03-1234 5678	+60 3-1234 5678

TIPS PENTING

Jika Flash Fill tidak mengesan pola dengan betul, taipkan **contoh kedua atau ketiga** untuk membantu Excel memahami corak.

Flash Fill **tidak dinamik**; jika data asal diubah, hasil Flash Fill tidak akan dikemas kini secara automatik.

Jika ciri ini tidak berfungsi, pastikan ia diaktifkan melalui **File > Options > Advanced > Automatically Flash Fill.**

★ FLASH FILL – BIAR EXCEL BUAT KERJA BERULANG, ANDA FOKUS PADA YANG PENTING! ★

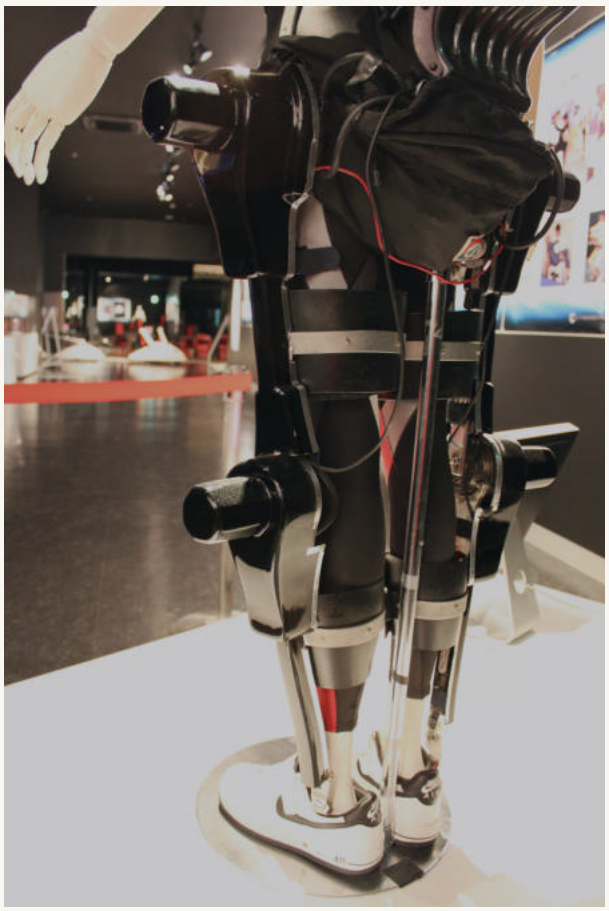
Oleh: Muhammad Rizal Bin Mohamad Amin

Dari Isyarat Otak ke Pergerakan Kaki: Kisah Teknologi Cybernic Voluntary Control System (CVCS)

Bagaimana isyarat tubuh yang halus menggerakkan robot pemulihan, menghubungkan niat manusia dengan langkah baharu yang penuh harapan.

Mungkin masih ramai yang tidak tahu Hospital Pakar USM (HUSM) ada menyediakan Perkhidmatan Rehabilitasi Robotik (Robo-Rehab). Perkhidmatan ini telah beroperasi secara rasmi pada bulan September 2020 lagi. Ia bermanfaat untuk rawatan pesakit yang memerlukan rawatan fizikal seperti pesakit strok, mereka yang mengalami kecederaan saraf tunjang atau kecederaan Brachial Plexus, sakit belakang dan kecederaan otak.

Peralatan yang digunakan dalam Robo-Rehab dikenali sebagai Hybrid Assistive Limb (HAL) dihasilkan oleh Cyberdine Inc.



HAL di Cyberdyne Studio, Jepun, 2010.
Foto: Yuichiro C. Katsumoto / CC BY 2.0.

Mengenali HAL

HAL ialah sut eksoskeleton (robot luaran) berfungsi untuk membantu proses pemulihan dalam meningkatkan keupayaan otot dan sendi pesakit supaya dapat berfungsi semula.

HAL menggunakan Teknologi Cybernic Voluntary Control System (CVCS), bidang sains yang melahirkan teknologi tersebut ialah Cybernics.

> *"Teknologi Cybernic Voluntary Control System (CVCS) sedikit sebanyak telah membuka ruang pemulihan dan harapan kepada mereka."*

Bagaimana Teknologi CVCS berfungsi ?

1. Isyarat Minda: Apabila seseorang hendak menggerakkan kaki, otak akan menghantar isyarat elektrik (isyarat bio-elektrik atau BES) melalui saraf tunjang ke otot.

2. Pengesan HAL: Walaupun otot pesakit terlalu lemah untuk bergerak, isyarat BES yang bocor di permukaan kulit akan dikesan oleh sensor khas yang terdapat pada HAL.

3. Maklum Balas Cybernic: Komputer HAL (menggunakan algoritma Cybernics) akan mentafsir isyarat tersebut dalam sekelip mata dan menggerakkan motor HAL untuk membantu kaki pesakit melangkah mengikut niat asalnya.

4. Proses Pembelajaran Otak: Apabila kaki bergerak, penderia pada HAL menghantar maklum balas sensori semula ke otak. Proses ini melatih semula otak pesakit (neuroplasticity) untuk belajar berjalan semula.

Mengenai Cybernics

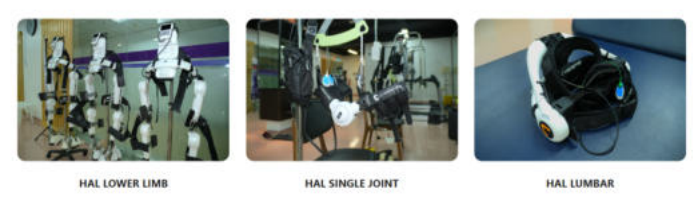
Cybernics adalah bidang Sains Multidisiplin diasaskan Prof. Yoshiyuki Sankai dari Universiti Tsukuba, Jepun. Ia adalah gabungan :

1. Sains Cybernetics
2. Sains Robotik
3. Sains Komputer terutama AI
4. Sains Neuro (neuroscience)
5. Sains tingkah laku (behavioral science)

Objektif utama Cybernics adalah untuk mencipta sistem mekanikal yang boleh berinteraksi, berkomunikasi dan berkoordinasi secara langsung dengan sistem saraf manusia.

> *"Objektif utama Cybernics adalah untuk mencipta sistem mekanikal yang boleh berinteraksi, berkomunikasi dan berkoordinasi secara langsung dengan sistem saraf manusia."*

TIGA BENTUK HAL



Sebagai contoh HAL LOWER LIMB mampu membantu pemulihan berjalan, berdiri dan duduk dengan stabil.

HAL LUMBAR pula boleh membantu rawatan menguatkan otot belakang dan meningkatkan kestabilan badan.

HAL SINGLE JOINT membantu menguatkan otot tangan dan kaki serta mengawal sendi siku dan lutut.

Sumbangan Sains Komputer dalam bidang Sains Cybernics

Sains Komputer terutama AI boleh diibaratkan sebagai otak dan sistem saraf dalam Cybernics. Tanpa teknologi tersebut, Sistem Cybernatics tidak boleh berfungsi secara masa nyata (real time).

Berikut adalah sumbangan kritikal Sains Komputer dan AI dalam bidang Cybernics:

1. Mentafsir Isyarat Otak dan Otot (Biosignal Processing)

Apabila manusia berniat untuk bergerak, otak menghantar isyarat bio-elektrik (BES) yang sangat lemah dan bercampur dengan "hingar"(noise) biologi yang lain. Algoritma Pembelajaran Mesin (Machine Learning) digunakan untuk menapis, menganalisis, dan mengecam corak isyarat bio-elektrik (BES) yang unik bagi setiap individu.

Hasilnya AI boleh membedah isyarat tersebut untuk mengetahui sama ada pengguna mahu melangkah, berdiri atau mengangkat tangan walaupun isyarat tersebut tersangat lemah (contohnya pada pesakit strok).

2. Kawalan Robotik Hibrid (Cybernic Control Autonomous vs. Voluntary)

Sains Komputer menyumbang dari sudut perisian untuk mengawal robot seperti HAL. Sistem ini menggabungkan dua kaedah kawalan:

• Kawalan Sukarela (Voluntary Control): Sistem komputer memproses isyarat saraf pengguna untuk menggerakkan robot mengikut kehendak pengguna.

• Kawalan Autonomi (Autonomous Control): Jika pesakit mempunyai kecederaan saraf yang parah sehinggakan tiada isyarat saraf dikesan, AI kawalan robotik akan mengambil alih secara automatik untuk menggerakkan kaki mengikut corak berjalan manusia yang normal.

Melalui sistem perisian ini, peralihan dan gabungan antara dua sistem kawalan ini berlaku dengan lancar tanpa gangguan (seamless integration).

3. Maklum Balas Biometrik Interaktif (Interactive Biofeedback)

Cybernics bukan sahaja tentang menggerakkan robot tetapi melatih semula otak manusia (neuroplasticity).

Sistem komputer boleh mencipta gelung maklum balas (feedback loop). Apabila robot bergerak, sensor pada robot menghantar data pergerakan kembali ke komputer dan seterusnya diselaraskan dengan pencerapan sensori pesakit.

Komputer memastikan visual, pergerakan fizikal dan tindakbalas saraf berlaku pada milisaat yang sama supaya otak menyedari, "Oh, saya sedang berjalan," sekaligus mempercepatkan penyembuhan saraf.

4. Penyesuaian Automatik (Adaptive Learning / Pembelajaran Adaptif)

Setiap pesakit mempunyai tahap kecederaan, berat badan dan gaya berjalan yang berbeza. Malah tahap keletihan pesakit juga berubah-ubah semasa sesi terapi. AI menggunakan pembelajaran adaptif untuk melaras kuasa motor robotik secara masa nyata.

Jika AI mengesan otot pesakit mula penat (berdasarkan perubahan isyarat elektrik), AI akan meningkatkan bantuan tork (kuasa) robot secara automatik.

> *“Cybernics bukan sahaja tentang menggerakkan robot tetapi melatih semula otak manusia (neuroplasticity).”*

Ruang pemulihan, ruang harapan

Bagi kebanyakan orang menggerakkan kaki untuk berjalan adalah hal biasa tetapi bagi mereka yang diuji dengan masalah kesihatan ia adalah sebuah perjuangan yang panjang. Teknologi Cybernic Voluntary Control System (CVCS) sedikit sebanyak telah membuka ruang pemulihan dan harapan kepada mereka.

Sumber :

1. https://hpusm.usm.my/perkhidmatan-kemudahan/perkhidmatankorporat/perkhidmatan-rehabilitasi-robotik-robo-rehab

2. https://www.cyberdyne.jp/en/

PROJEK Wi-Fi IPTA

KAMPUS KEJURUTERAAN USM

Tuanku Syed Sirajuddin • Nibong Tebal



740

TITIK AKSES TAMBAHAN

Disediakan di Kampus Kejuruteraan melalui Fasa 3

GARIS MASA FASA 3

5 hari lebih awal

18 September 2026
Siap dilaksanakan

23 September 2026
Sasaran asal

STATUS NAIK TARAF ASRAMA

TELAH SIAP
SH1 • SH2 • SH3 • SH4 • SH6

SH5
Akan dilaksanakan sebelum akhir tahun 2026

TUJUAN PROJEK

- Memperkukuh ketersambungan digital
- Menyokong pembelajaran dan kehidupan kampus
- Meningkatkan kapasiti dan kualiti capaian Wi-Fi

INISIATIF

Kementerian Komunikasi melalui MCMC
Projek Pemberian Perkhidmatan Sejagat (USP)

UNIVERSITI SAINS MALAYSIA

PUSAT TRANSFORMASI DIGITAL





ATTENTION!!!

DON'T USE PIRATE SOFTWARE

Article 4.3.15 of USM's Information Technology Policy: All software obtained must be legitimate or licensed and used according to the terms set by the supplier or manufacturer. The use of any software is the responsibility of the user.



Buying software at an unreasonable price from an online shopping is vulnerable to buying pirate software.

PTD reserves the right to block internet access to computers detected using pirate software

Pirate software is software that has been copied and distributed without permission from the copyright owner. The use of pirate software can be prosecuted under the Copyright Act 1987. Students who use pirate software can be sued by the licensee. The University is not responsible for the suit.

UNIT KESELAMATAN ICT

PUSAT TRANSFORMASI DIGITAL
USM KAMPUS KEJURUTERAAN
TUANKU SYED SIRAJUDDIN

BIT OF BYTE

MAGAZINE 2026

Digital @USM

PUSAT TRANSFORMASI DIGITAL
USM KAMPUS KEJURUTERAAN
TUANKU SYED SIRAJUDDIN

digital.eng.usm.my