



UPM
UNIVERSITI PUTRA MALAYSIA
BERILMU BERBAKTI



Pameran **CAKNA** **KESELAMATAN SIBER**



PERPUSTAKAAN SULTAN ABDUL SAMAD
UNIVERSITI PUTRA MALAYSIA

Sumber:



The Government of Malaysia's Official Gateway
MyGovernment

AGRICULTURE . INNOVATION . LIFE

BERILMU BERBAKTI I
WITH KNOWLEDGE WE SERVE
www.lib.upm.edu.my | www.upm.edu.my



KESELAMATAN SIBER

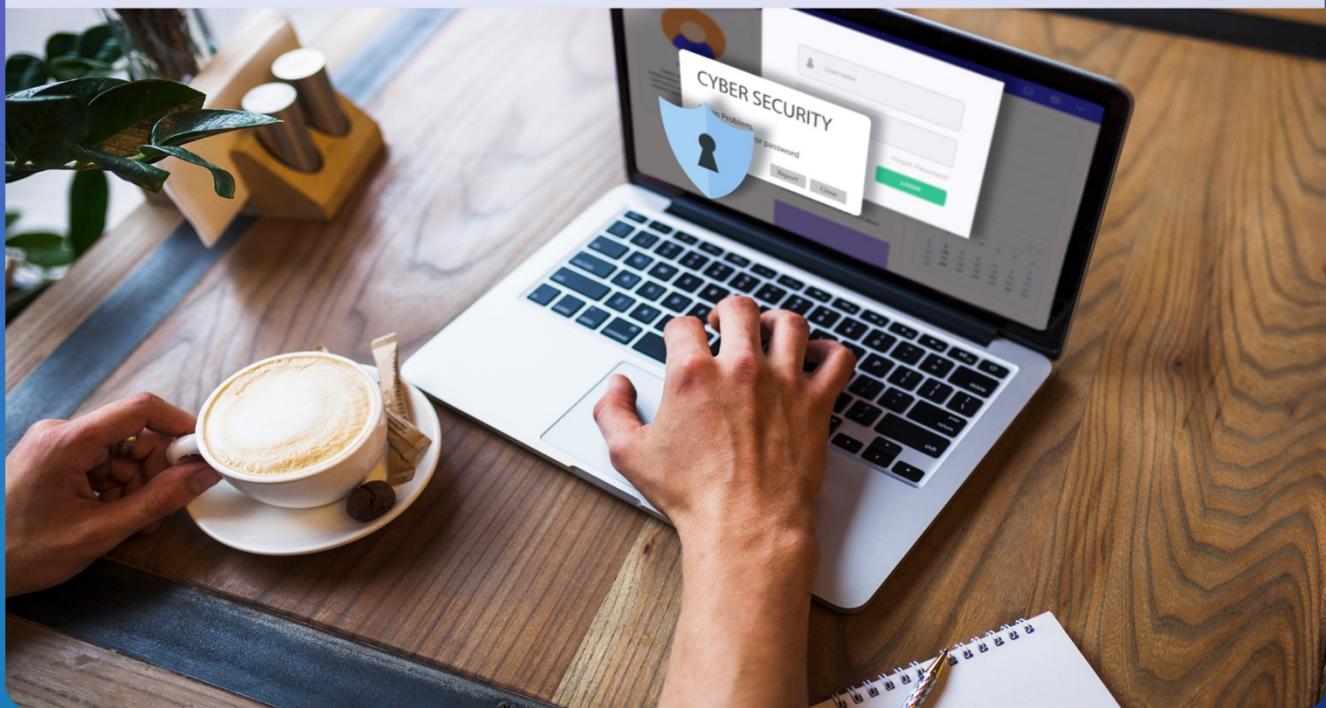
Keselamatan siber merujuk kepada teknologi, proses dan amalan dalam melindungi rangkaian, peranti atau data daripada serangan atau kerosakan disebabkan penjenayah (Nate Lord, 2017).

Ia juga merupakan perbuatan melindungi keselamatan maklumat dan ruang siber daripada ancaman anasir luar (George, 2017). Perkara ini termasuk amalan-amalan pengguna Internet untuk melindungi diri dari ancaman-ancaman siber ketika melayari atau menggunakan Internet.

Ia penting dalam memupuk pengetahuan tentang keselamatan siber dan kesedaran keselamatan internet demi mewujudkan budaya penggunaan internet yang positif di kalangan pengguna Internet.

Sumber:

1. Nate Lord. (2017). What is Cyber Security.
<https://digitalguradian.com/blog/what-cyber-security>
2. George, C. (2017). The EU's Approach to Cybersecurity.
http://repository.essex.ac.uk/19872/1/EU-Japan_9_Cyber_Security_Chrisou_EU.pdf



KATEGORI ANCAMAN SIBER



PENCEROBOHAN (INTRUSION)

Insiden pencerobohan sistem dan aplikasi komputer tanpa kebenaran dan berupaya mengubah kandungan sistem tersebut.



PENIPUAN (FRAUD)

Merujuk kepada skim penipuan yang menggunakan satu atau lebih komponen internet dan telekomunikasi termasuklah ruangan chat, e-mel, papan buletin, laman web dan sms untuk mewujudkan ruangan pembujukan dan transaksi wang seperti laman web atau e-mel yang menyerupai atau kelihatan seperti badan kewangan atau syarikat yang sahih beroperasi (phishing), pelaburan e-dagang atau skim piramid.



GANGGUAN (HARASSMENT)

Melibatkan penghantaran mesej, gambar dan video yang berunsur fitnah, lucah, gangguan dan ancaman kepada pengguna lain.



ANCAMAN PENCEROBOHAN (HACK THREAT)

Merangkumi serangan ke atas sistem dan aplikasi komputer agensi-agensi tertentu dengan tujuan melumpuhkan operasi sistem dan aplikasi komputer bagi agensi berkenaan.



KOD BERBAHAYA (MALICIOUS CODE)

Merupakan perisian atau skrip komputer yang diprogramkan untuk menceroboh komputer dan merosakkan sistem. Kod berbahaya termasuklah skrip serangan, virus, worm, Trojan horse, program Back door dan kandungan aktif berbahaya.



GANGGUAN PERKHIDMATAN (DENIAL OF SERVICE)

Merupakan serangan ke atas sesuatu sistem atau aplikasi komputer yang menyebabkan para pengguna tidak dapat mencapai dan menggunakan sistem atau aplikasi berkenaan.

MyCERT
Malaysia Cyber Emergency Response Team

SCAN ME



#	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Spam	10	4	11	5	8	4	7	6	6	14	13	14	102
Intrusion	178	252	119	100	116	112	126	101	94	102	54	56	1,410
Vulnerabilities Report	8	5	12	4	6	3	3	13	3	4	3	5	69
Intrusion Attempt	11	10	16	12	24	18	9	12	12	8	12	15	159
Denial of Service	1	2	3	1	3	0	1	2	3	0	4	2	22
Malicious Codes	58	44	42	29	83	64	44	25	76	53	60	70	648
Content Related	2	11	10	6	9	5	8	7	12	12	3	6	91
Fraud	746	502	566	726	689	861	639	690	490	473	365	361	7,098
	1,049	867	819	912	968	1,122	878	880	731	696	539	555	10,016

Jadual 1: Insiden Keselamatan Siber Tahun 2021 oleh MyCERT, CyberSecurity, Malaysia.

10 LANGKAH MUDAH KESEDARAN KESELAMATAN SIBER

Jenayah siber boleh melibatkan semua golongan dan anda perlulah menyedari apa yang perlu diperhatikan dan bagaimana melindungi diri anda daripada jenayah siber.

Ketahui langkah-langkah yang boleh di ambil untuk mengenali serangan siber dan seterusnya dapat mengelakkan diri dari menjadi mangsa virus, penipuan dan pancingan data. Berikut adalah 10 langkah mudah kesedaran keselamatan siber yang boleh dipraktikkan bersama:

1



Gunakan KATA LALUAN

- Gunakan kata laluan yang kreatif (gabungan huruf, nombor dan simbol).
- Elakkan daripada mendedahkan kata laluan kepada orang lain.
- Sentiasa tukar kata laluan secara berkala dan elakkan daripada menggunakan kata laluan yang sama (berulang).
- Sulitkan (encrypt) penghantaran dokumen rasmi Kerajaan dengan kata laluan.
- Elakkan menghantar kata laluan bersama-sama dengan dokumen rasmi Kerajaan.

2



KEMASKINI perisian keselamatan

- Lengkapkan komputer dan gajet dengan perisian keselamatan (seperti anti-virus dan anti-spyware) terkini.
- Elakkan daripada menggunakan perisian keselamatan yang telah tamat tempoh.
- Gunakan perisian tulen.

3



SIMPAN dan LINDUNGI maklumat

- Elakkan daripada memuat naik dokumen rasmi Kerajaan dalam public cloud.
- Sentiasa imbas peranti storan sebelum menggunakan.
- Sentiasa sediakan salinan pendua (back up) maklumat digital secara berkala.
- Elakkan daripada meninggalkan komputer dan gajet tanpa sebarang pengawasan.
- Putuskan sambungan Internet atau wi-fi sekiranya tidak menggunakan lagi.
- Pastikan meja kerja dikemas dan semua maklumat rasmi (termasuk yang berada di dalam peranti storan) disimpan di tempat yang selamat dan berkunci.

10 LANGKAH MUDAH KESEDARAN KESELAMATAN SIBER

4



ELAK terpedaya

- Elakkan daripada terus mempercayai kandungan laman web, blog dan e-mel yang diragui atau daripada orang yang tidak dikenali.
- Semak dan rujuk kepada sumber-sumber yang sahih.

5



BERETIKA menggunakan internet dan media sosial

- Pastikan alamat e-mel dan kata laluan rasmi tidak digunakan dalam akaun peribadi media sosial.
- Keluar (log out) daripada akaun media sosial apabila tidak digunakan lagi.
- Elakkan daripada berkongsi maklumat peribadi dan maklumat berkaitan tugas rasmi di internet dan media sosial.
- Elakkan daripada memuat turun aplikasi yang tidak diketahui tahap keselamatan.
- Elakkan daripada menggunakan media sosial untuk tujuan peribadi semasa waktu pejabat.
- Berhati-hati menggunakan media sosial untuk tujuan peribadi supaya tidak mendedahkan sebarang maklumat rasmi.
- Elakkan daripada membuat sebarang komen mengenai isu-isu yang melibatkan agensi/organisasi atau yang berbentuk serangan peribadi.
- Pastikan perkongsian dan penggunaan maklumat yang berkaitan dengan hak cipta dan harta intelek telah mendapat kebenaran terlebih dahulu daripada pihak yang berkenaan.
- Elakkan daripada menggunakan wi-fi umum yang tidak diketahui tahap keselamatan untuk melaksanakan kerja-kerja rasmi.
- Kenalpasti rakan media sosial anda.

6



WASPADA jenayah siber

- Jangan benarkan individu lain menggunakan identiti dan kata laluan akaun e-mel dan media sosial anda.
- Elakkan daripada melayari laman web dan blog yang berunsurkan lucah, fitnah, hasutan, skim cepat kaya dan ideologi keganasan.
- Elakkan daripada menyebarkan kandungan yang berunsurkan lucah, fitnah, hasutan, skim cepat kaya dan ideologi keganasan.
- Jangan mudah terpedaya dengan tawaran atau maklumat daripada individu yang tidak dikenali yang menghubungi anda melalui e-mel atau media sosial.

10 LANGKAH MUDAH KESEDARAN KESELAMATAN SIBER

7



FIKIR sebelum klik

- Jangan klik pada e-mel, pautan atau lampiran yang mencurigakan (termasuk dari orang yang tidak dikenali). Padamkan e-mel tersebut.

8



LAPORKAN

- Laporkan sebarang insiden kebocoran maklumat kepada pihak berkaitan.
- Laporkan dengan segera kehilangan sebarang aset ICT kerajaan (seperti peranti storan, komputer riba, komputer).
- Laporkan kepada pihak berkuasa sekiranya berlaku sebarang insiden jenayah siber seperti penipuan Internet.

9



AMBIL TAHU

- Peka dengan trend ancaman siber terkini.
- Peka, fahami dan waspada mengenai kesan-kesan negatif akibat penyalahgunaan Internet.

10



PATUHI

- Ketahui dan patuhi polisi, arahan, peraturan, garis panduan dan pekeliling berkaitan keselamatan siber yang dikeluarkan oleh agensi/organisasi anda dan Kerajaan.

Sumber: <https://www.nacsa.gov.my/doc/10LangkahMudah-v8.pdf>



TIPS KESEJAHTERAAN SIBER

SENTIASA SELAMAT DI DALAM TALIAN

Kenal pasti rakan siber anda kerana kadangkala mereka mungkin akan mengancam diri anda.

BERSUARA DAN LAPOR

Sekiranya anda berhadapan dengan aktiviti dalam talian yang mencurigakan, maklumkan kepada orang yang anda percaya atau lapor kepada pihak berkuasa.



HORMATI DIRI ANDA DAN ORANG LAIN DI DALAM TALIAN

Kongsi hanya perkara yang baik dan sentiasa waspada semasa membuat hantaran maklumat di dalam talian.

KEKAL BERHUBUNG DENGAN DUNIA SEBENAR

Luangkan masa dengan melakukan aktiviti fizikal dan bergembira bersama keluarga serta rakan taulan.

TETAPKAN MATLAMAT PENGGUNAAN INTERNET

Berehat sekurang-kurangnya 5 minit setiap jam untuk melakukan aktiviti fizikal. Belajar untuk menghargai dunia sebenar.

Sumber:

<https://www.pdp.gov.my/jpdv2/awam/tips-keselamatan-cyber/?lang=en>



MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

||CyberSecurity||
MALAYSIA

GUNA INTERNET SECARA BERHEMAH.

ELAK DARI MENJADI MANGSA SALAH LAKU INTERNET



Jika anda menghadapi ancaman dan insiden keselamatan siber, laporan ke Pusat Bantuan Kecemasan Cyber999 melalui saluran berikut:

Cyber999

No. Kecemasan:
1-300-88-2999 (9.00 pagi - 9.00 petang)

Emel:
cyber999@cybersecurity.my

Mobile:
+6019-266 5850 (24 jam)

SMS:
CYBER999 REPORT (email)(complaint) to 15888

Cyber999 App:
Muat turun di App Store/Google Play

Borang Atas Talian:
<https://www.mycert.org.my>



@CyberSecurityMalaysia



@cybersecuritymy



cybersecurity_malaysia



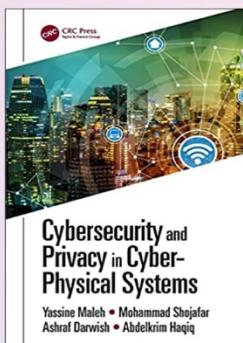
CyberSecurity Malaysia



CyberSecurityMy

BACAAN TAMBAHAN

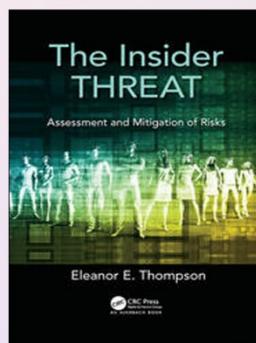
BUKU



Cybersecurity and privacy in cyber physical systems

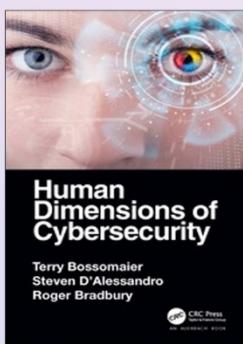
Yassine Maleh, Shojafar
Mohammad, Darwish Ashraf,
Haqiq Abdelkrim.

scan me



**The insider threat :
assessment and mitigation of
risks**

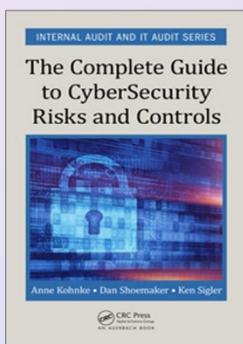
Eleanor E. Thompson.



**Human dimensions of
cybersecurity**

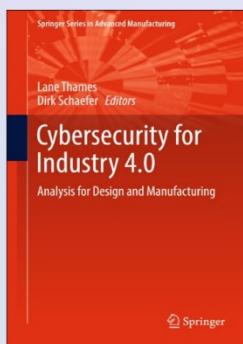
Terry Bossomaier, Steven
D'Alessandro, Roger Bradbury.

scan me



**The complete guide to
cybersecurity risks and
controls**

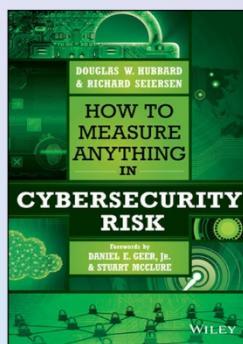
Anne Kohnke, Dan Shoemaker,
Ken Sigler.



**Cybersecurity for industry
4.0. analysis for design and
manufacturing**

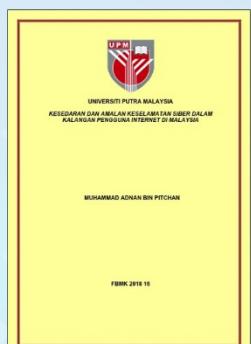
Lane Thamess, Dirk Schaefer,
editors.

scan me



**How to measure anything in
cybersecurity risk**

Douglas W. Hubbard,
Richard Seiersen.



**Kesedaran dan amalan
keselamatan siber dalam
kalangan pengguna internet
di Malaysia**

Muhammad Adnan Pitchan.

scan me



BACAAN TAMBAHAN

ARTIKEL JURNAL



Pitchan, M. A., & Omar, S. Z. (2019). **Dasar Keselamatan Siber Malaysia: Tinjauan Terhadap Kesedaran Netizen dan Undang-Undang.** *Jurnal Komunikasi: Malaysian Journal of Communication*, 35, 103-119.



Yusuf, S., Idris, K., Samah, A. A., Ibrahim, A., Ramli, N. S., Ibrahim, M. S., & Rahman, N. A. A. (2020). **Keyboard Warrior, Online Predator or Cyber Bully? The Growing Menace of Child Exposure to Internet Harm based on Research Evidence.** *Pertanika Journal of Social Sciences & Humanities*, 28(2).



Pitchagan, M. A., Omar, S. Z., & Ghazali, A. H. A. (2019). **Amalan Keselamatan Siber Pengguna Internet terhadap Buli Siber, Pornografi, E-Mel Phishing dan Pembelian dalam Talian.** *Jurnal Komunikasi: Malaysian Journal of Communication*, 35(3), 212-227.



Mohammad, T., Hussin, N. A. M., & Husin, M. H. (2022). **Online safety awareness and human factors: An application of the theory of human ecology.** *Technology in Society*, 68, 101823.



Faith, B. F., Hamid, S., Norman, A., Johnson, O. F., & Eke, C. I. (2020, March). **Relating Factors of Tertiary Institution Students' Cybersecurity Behavior.** In *2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS)* (pp. 1-6). IEEE.



Wahid, S. D. M., Buja, A. G., Jono, M. N. H. H., & Aziz, A. A. (2021). **Assessing the influential factors of cybersecurity awareness in Malaysia during the pandemic outbreak: A structural equation modeling.** *International Journal of Advanced Technology and Engineering Exploration*, 8(74), 73.



Bakar, N. A., Mohd, M., & Sulaiman, R. (2017, November). **Information leakage preventive training.** In *2017 6th International Conference on Electrical Engineering and Informatics (ICEEI)* (pp. 1-6). IEEE.



Abdalla, M., & Arshad, Y. **Information Security: Cybersecurity Standards Adoption Among Malaysian Public Listed Companies.**

Pameran
CAKNA
KESELAMATAN SIBER

PERPUSTAKAAN SULTAN ABDUL SAMAD
UNIVERSITI PUTRA MALAYSIA