www.mot.gov.my

KEMENTERIAN PENGANGKUTAN MALAYSIA

Buletin ICT MOT

BIL. 3/2017 (Disember)

SEBENARNYA.MY
[redacted] Tidak Pasti Jangan Kongsi

BAGAIMANA UNTUK MELINDUNGI TERHADAP RANSOMWARE!

PASUKAN BAHAGIAN PENGURUSAN MAKLUMAT MENANG TEMPAT KE-2 PERTANDINGAN HACKATHON 24 JAM APLIKASI MUDAH ALIH 2017.

SAFE INTERNET BANKING

CyberSecurity MALAYSIA
An agency under MOSTI

ISTILAH ICT BIL. 13 HINGGA 19

DASAR KESELAMATAN ICT

DKICT

BAGAIMANA MENJADIKAN AKAUN INTERNET ANDA LEBIH SELAMAT

Penaung:
EN MOHD KADRI IBRAHIM

Editor:
PN ROSLIZA HAMZAH

Sumbangan Bahan:

PN ROSLIZA HAMZAH
EN SURIZALMAN MOHD ZAIN
EN SUBRAMANI A/L PAIDUTHALY
PN NOR FAZILLAH MOHD MASRI
EN RAMLEE ATAN
CIK NORZIE NANI ABDUL SAMAD
PN NURUL NAJWA SAMSUDDIN
PN IZZIANA BAHADUN
PN ROSLINDA SANI
PN NOR AINI ABDULLAH
EN MIOR AHMAD FITRI SELIPOL BAHRI
EN SYAFIQ NOR ABIDIN

Diterbitkan oleh:
BAHAGIAN PENGURUSAN MAKLUMAT,
ARAS 7, KEMENTERIAN PENGANGKUTAN MALAYSIA,
NO. 26, JLN. TUN HUSSEIN, 62100 W.P. PUTRAJAYA.

KEMENTERIAN PENGANGKUTAN MALAYSIA

Buletin ICT MOT

BIL. 3/2017 (Disember) www.mot.gov.my

DASAR KESELAMATAN ICT

DKICT

APA ITU DKICT?

Mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Dasar ini diguna pakai oleh MOT dan agensi-agensi di bawahnya.

Dasar ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT.

OBJEKTIF UTAMA

1. Memastikan kelancaran operasi MOT dan meminimumkan kerosakan atau kemusnahan
2. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, ketersediaan, kesahihan maklumat dan komunikasi
3. Mencegah salah guna atau kecurian aset ICT Kerajaan

8 PRINSIP

1. **AKSES ATAS DASAR PERLU MENGETAHUI**
Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut.

2. **HAK AKSES MINIMUM**
Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja.

3. **AKAUNTABILITI**
Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT.

4. **PENGASINGAN**
Tugas mewujud, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi.

5. **PENGAUDITAN**
Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan.

6. **PEMATUHAN**
DKICT MOT hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT

7. **PEMULIHAN**
Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan

8. **SALING BERGANTUNGAN**
Setiap prinsip di atas adalah saling lengkap-melengkapi dan bergantung antara satu sama lain.

KEMENTERIAN PENGANGKUTAN MALAYSIA

Buletin ICT MOT

BIL. 3/2017 (Disember)

www.mot.gov.my

SEBENARNYA.MY
Tidak Pasti Jangan Kongsi

Kebangkitan teknologi, kepantasan mesej, video dan gambar yang ditular adalah hakikat dan cabaran yang harus ditempuhi dalam menangani budaya tular palsu bagi mengelakkan ia menjadi lebih parah dalam masyarakat.

Tidak kira sama ada menerusi Facebook mahupun mesej berantai yang dikongsi melalui WhatsApp, budaya tular kian meresap ke dalam jiwa pengguna masa kini menyebabkan apa saja perkara yang belum tentu kesahihannya, dikongsi dengan pantas.

Portal **SEBENARNYA.MY** dibangunkan Suruhanjaya Komunikasi dan Multimedia (SKMM) dengan kerjasama agensi-agensi kerajaan dan telah dilancarkan pada Mac 2017.

Portal **SEBENARNYA.MY** adalah sebuah pusat sehenti bagi rakyat Malaysia untuk menyemak dan melapor berita yang tidak ditentusahkan, yang diterima secara dalam talian melalui platform media sosial, perkhidmatan mesej segera, blog, laman sesawang, dan lain-lain.

Dengan adanya portal ini diharap gejala penularan berita palsu dalam talian yang boleh memberi kesan kepada masyarakat dan negara, dapat ditangani dengan berkesan.

KEMENTERIAN PENGANGKUTAN MALAYSIA

Buletin ICT MOT

BIL. 3/2017 (Disember)

www.mot.gov.my

BAGAIMANA UNTUK MELINDUNGI TERHADAP RANSOMWARE?

STOP | THINK | CONNECT

TIPS KESELAMATAN SIBER #4

Jangan buka emel yang mencurigakan. Semak alamat penghantar sebelum membuka sebarang pautan atau muat turun daripada emel

Pastikan perisian keselamatan sentiasa dikemaskini dengan signature virus terkini

Jangan melayari laman yang mencurigakan

Sentiasa kemaskini patches terkini pada perisian, sistem dan plug-ins

Sentiasa backup data dan simpan secara offline. Amalkan syarat 3-2-1: 3 salinan data dalam, 2 media storan berbeza, dan salah satu dismpan pada lokasi offsite. Uji backup untuk pastikan ia dapat dipulihkan semula dengan berjaya.

Sekiranya tidak perlu jangan aktifkan macro dalam perisian office

Hadkan kebenaran menulis (write permission) pada fail server

Bookmark laman yang kerap dikunjungi dan selamat untuk elakkan dari menaip alamat yang salah

Guna perisian keselamatan web dan emel untuk sekat akses ke laman merbahaya serta dapat mengimbas semua fail dimuat turun

Gunakan endpoint protection yang boleh mengenalpasti variasi malware dan aliran trafik luar biasa

Elakkan pelaksanaan fail dalam folder sementara (temporary)

Sekiranya disyaki terdapat jangkitan, putuskan sambungan pada rangkaian dengan segera.

Jangan benarkan akses kepada maklumat atau pemacu rangkaian

Jangan membayar wang tebusan. Tiada jaminan akses kepada fail akan diperolehi semula.

Didik pengguna untuk melaporkan sebarang ancaman yang dikesan dan sentiasa berwaspada terhadap ancaman serta cara-cara pencegahan.

MyCERT Malaysia Computer Emergency Response Team

Cyber999

https://heimdalsecurity.com/blog/what-is-ransomware-protection/
https://heimdalsecurity.com/blog/ransomware-decryption-tools/

KEMENTERIAN PENGANGKUTAN MALAYSIA

Buletin ICT MOT

BIL. 3/2017 (Disember)

www.mot.gov.my

SAFE INTERNET BANKING

Keep your password/PIN code safe and memorize them. Make sure you change them regularly (at least every 3 months). If you conduct transactions in a number of websites, use different passwords for each. Create unique passwords that are difficult to guess, e.g. use combination of letters and numbers.

How do you know the website is secured?

- o Look for https:// in the URL and not http:// when you login
- o Look at the status bar for the security icon (locked padlock) when you visit the bank site. Ensure the icon is within the browser frame.

Web Browser	Secured	Not Secured
Microsoft Windows		
Internet Explorer		
Netscape Navigator		
Firefox		
Apple MAC		
Apple Safari		
Firefox		

When using a public computer, clear the browser cache, cookies and history once you complete your online transaction and logout (refer to you bank's website for online guidance). Make sure you logout properly after every Internet banking sessionand they must not just close the browser.

Be aware of your surrounding and never leave your computer unattended when you are conducting your transactions. If you are unsure of the security of the computer, do not use it for online transactions.

Use an antivirus, anti-spyware and personal firewall that is trusted and well supported by the vendor. Make sure the programs are regularly updated with the current version.

Make sure your PC and browser are updated with the latest patches/fixes.

Be sure that all email attachments are scanned with your anti-virus and are from trusted sources before opening them. Make sure you do not click on any links attached in your emails.

Do not respond to emails asking for personal information, login information or change password notification. If you are not sure of the sender, contact your bank.

If you decide to go to other websites linked via your internet banking website, read the privacy and policy information of that website first before conducting any online transactions.

Always check your account balances/statement to ensure that no unauthorized withdrawal has taken place.

When making any online payment, use a credit card. Credit cards usually have stronger protection for personal liability. Keep a copy of transaction receipt.

When visiting your online banking site, always check that the Date and Time, matches the date and time when you last signed in.

If your bank account has been compromised, act fast and inform the bank, or contact the Malaysia Cyber Security Centre (http://www.niser.org.my or http://www.mycert.org.my)

- o Tel – 03-89961901
- o Fax: 03-89960827
- o Email: mycert@mycert.org.my
- o SMS: 019-2813801
- o MyCERT 24x7 call incident reporting : 019-2665850

KEMENTERIAN PENGANGKUTAN MALAYSIA

Buletin ICT MOT

BIL. 3/2017 (Disember)

www.mot.gov.my

BAGAIMANA MENJADIKAN AKAUN INTERNET ANDA LEBIH SELAMAT

Akhir-akhir ini, kita sering mendengar berkaitan dengan ketirisan data disebabkan beberapa kelemahan teknologi, sekaligus membuatkan ramai pengguna risau akan mengenai keselamatan akaun internet mereka yang menyimpan pelbagai maklumat.

Untuk mengurangkan risiko, salah satu perkara yang boleh dilakukan semua pengguna adalah mengaktifkan sokongan pengesahan dwi-faktor. Kebanyakkan perkhidmatan web menyokongnya, dimana ia akan memerlukan pengguna memasukkan kata laluan seperti biasa dan kemudiannya turut memasukkan satu kod tambahan yang akan dihantar terus ke peranti mudah-alih anda ataupun ditawarkan melalui status aplikasi khusus untuk pengguna.

AKAUN GOOGLE

Google memanggil sokongan ini sebagai "2-Step Verification". Dengan mengaktifkan sokongan ini, ia akan memautkan akaun Google anda kepada nombor telefon peribadi anda, dimana setiap kali ingin log masuk daripada suatu computer atau peranti tidak dikenali, anda akan diminta untuk memasukkan suatu kod rawak yang dihantar ke peranti mudah-alih anda dalam bentuk SMS.

AKAUN FACEBOOK

Untuk fungsi yang sama, pihak Facebook memanggilnya sebagai Login Approvals. Sama seperti apa yang ditawarkan oleh Google, pihak Facebook turut menghantar SMS berbentuk suatu angka rawak untuk pengguna untuk dimasukkan ketika log masuk ke akaun Facebook mereka.

Selain bentuk SMS, sekiranya anda mempunyai aplikasi Facebook terpasang pada peranti mudah-alih anda, ia turut akan memberikan pilihan untuk menghantar kod melaluinya yang mana berfungsi lebih pantas berbanding dengan penghantaran SMS. Untuk mengaktifkannya, pengguna hanya perlu ke halaman Settings, dan memasukkan nombor telefon dan beberapa maklumat tambahan pada Login Approvals.

AKAUN TWITTER

Twitter turut menawarkan sokongan yang sama menyerupai Facebook, dimana pengguna boleh menggunakan sokongan SMS ataupun menggunakan aplikasi untuk menawarkan kod rawak untuk digunakan ketika log masuk ke perkhidmatan mereka. Untuk mengaktifkannya, pengguna hanya perlu ke halaman Security di Twitter.com, da kemudian mengaktifkan ia pada bahagian Login Verification.

AKAUN MICROSOFT

Dengan penggunaan akaun Microsoft pada Windows 8, Windows Phone, Skype, OneDrive dan sebagainya, akaun Microsoft kini turut menjadi salah satu akaun utama yang digunakan ramai pengguna di web. Microsoft tidak mempunyai sebarang nama khusus untuk fungsi ini. Untuk mengaktifkannya, pengguna hanya perlu ke halaman akaun Microsoft mereka dan klik pada "Security Info".

Sumber : Aman Firdaus, Majalah PC

KEMENTERIAN PENGANGKUTAN MALAYSIA

Buletin ICT MOT

BIL. 3/2017 (Disember)

www.mot.gov.my

CyberSecurity MALAYSIA

An agency under MOSTI

- Delete any messages of those who leave inappropriate comments.
- Use the privacy settings feature of the social networking site. It can help to protect your information and your friend's information. Set the "privacy" function so that people can only be added as your friend and view your profile if you approve it.
- Do not post information about your friends as you could put them at risk.
- Do remember what you post online is not private. Parents, teachers, and employers, may go online and find out about you.

As for parents to help their kids to use social networking sites safely

Kids and teenagers are seen to be more tech-savvy than their parents today. They are exposed to computers and internet in school but may not know the safety tips on various web applications they use that range from, email, chat rooms, online gaming and more. Parents cannot neglect their children while they are online and need to advise their children just like in real life, especially when dealing with strangers and giving information to others. Stalkers and other criminal are using website containing personal information to lure their victims, which kids are ever willing to post their information online without realizing the dangers. Kids find that social networking site as a platform to increase their circle of friends, apart from friends at school or their neighborhood.

The following are some tips for educating your children on making friends online safely:

- Monitor their activities on the Internet. You can monitor by installing some monitoring software to watch their online activities, e.g website they visit.
- They need to know what information should be kept private and not shared. Educate them on why such information should not be revealed. Citing real case scenarios or giving examples on what might happen can make kids look at it seriously.
- Tell them to inform you if someone asks or talks about sensitive issues or something that makes them feel uncomfortable.
- They should only post information that they or you feel comfortable with. Make sure that they understand the risks of posting personal information on these sites.
- Tell them the information they post online cannot be taken back.
- Enable privacy settings on the website to restrict who can post and access information on your child's site.
- Report to the site if you reasonably believe that someone is a scam artist or sexual predator on your children's profile site or on the social networking site in general.

INCIDENT REPORTING CHANNELS

Online Reporting
http://www.mycert.org.my/report_incidents/online_form.html

Telephone
Call Cyber999 Hotline number at 1-300-88-2999 or +603-8992 6969.
Office Hours only. Monday – Friday, 8:30am - 5:30pm, GMT+0800

Mobile Phone
Call +6019-266 5850 (24 x 7)

SMS
Send SMS to +6019-281 3801

Email
Send email to mycert@mycert.org.my

Fax
Download form at:
http://www.mycert.org.my/en/services/report_incidents/fax_details/main/detail/157/index.html and fax to +603-8945 3442

CyberSecurity Malaysia
Level 7, Sapura @ Mines, 7, Jalan Tasik
The Mines Resort City, 43300 Seri Kembangan
Selangor Darul Ehsan, Malaysia.
Tel : +603 - 8992 6888 Fax : +603 - 8945 3205
E-mail : info@cybersecurity.my
www.cybersecurity.my

MOSTI
Ministry of Science, Technology and Innovation

Best Brand Internet Security

ISMS SIRIM

INFORMATION SECURITY BEST PRACTICE SERIES:

SOCIAL NETWORKING

CyberSecurity MALAYSIA

An agency under MOSTI

KEMENTERIAN PENGANGKUTAN MALAYSIA

Buletin ICT MOT

BIL. 3/2017 (Disember)

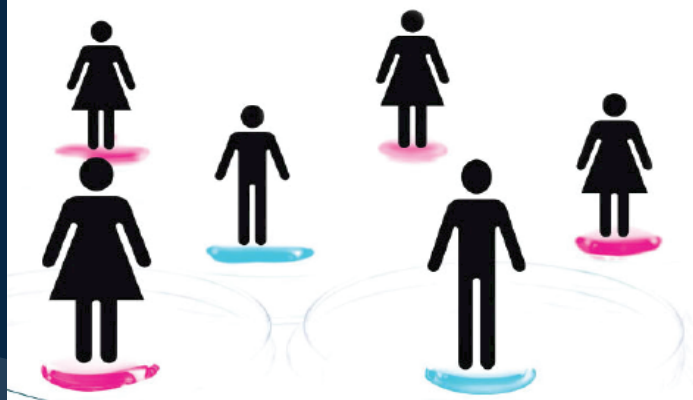
www.mot.gov.my

CyberSecurity MALAYSIA

An agency under MOSTI

Social networking has revolutionized the way people communicate, exchange information and participate in activities that explores interest of others.

Social networking has revolutionized the way people communicate, exchange information and participate in activities that explores interest of others. People with shared thoughts and interest come together in this ever growing medium. Social networking websites also employ the use of email and instant messaging services.



This platform enables people from near and far to communicate with their families, colleagues and friends. This platform has also opened up opportunities for businesses and entrepreneurs to build their contact database and use it as means to serve their customers. They can also promote their products and services using banner and text ads. Social networking websites are also widely used to network professionals together for meetings and information sharing.

Since social networking websites are laden with personal information and there have been growing concerns with people giving out too much of their personal information that gives cyber criminals opportunity to lure victims. Who needs to hack or dumpster dive when all they need to do is turn on the PC and log on to a social networking site. Social networking sites such as MySpace and Facebook have become an attractive target for cybercriminals looking to mine personal information, to trick users with phishing scams and spreading malware on exploited profile sites.

Yes, these sites are taking necessary steps by implementing security measures to minimize this problem, but users must still be cautious and aware. Necessary steps have to be taken by every user to protect themselves and their computer from threats as this involves their personal information and also information of their associates. They cannot just depend on the social networking sites to be responsible and do the job for them.

If that were not enough, time wasting and internet addiction can be another major setback resulting from these social networking sites. Children and teenagers, and even working adults may spend hours online modifying their profiles and communicating with others. Tasks and productivity may suffer as a result. Not to forget cyber bullying in which many websites let you rate another member's profile. This opens the opportunity for cyber bullying and allows nasty comments to be made. Negative comments can also appear in discussion groups and blogs.

The objective of this best practice is to provide useful safety tips to end users on the common threats and precautionary measures of social networking sites. On these sites, people usually share and exchange information, photos, videos, personal information, play online games, participate in interest groups, share thoughts, organize events, etc. It is one of the most engaging web applications of today as it is people-centric.

Tips to be safe when making friends online

- Beware of pretender and be vigilant. Potential exploiters can pretend to be someone else with a different age and background and convince you to add them as your "friend".
- Never share or post your personal information such as hand phone number, home/ work address in your profile. Potential exploiters use these profiles to search for victims.
- Be careful when posting text and image as it can be copied out by potential exploiter and in some cases, it cannot be taken back. Think before posting your photos as exploiter can use it to blackmail or threaten you. Personal photos should not have revealing information, e.g. your location.
- Never share your password with anyone.
- Add people as friends to your site only if you know them in person. Do not meet someone whom you have first "met" on a social networking site. People may not be who they say they are and this could put you in potential danger.
- Do not respond to harassing or threatening comments posted on your profile.

KEMENTERIAN PENGANGKUTAN MALAYSIA

Buletin ICT MOT

BIL. 3/2017 (Disember) www.mot.gov.my

PASUKAN BAHAGIAN PENGURUSAN MAKLUMAT MENANG TEMPAT KE-2 PERTANDINGAN HACKATHON 24 JAM APLIKASI MUDAH ALIH 2017.

Pada 11-13 September 2017, MAMPU telah mengadakan pertandingan Hackathon 24 Jam Aplikasi Mudah Alih 2017 dan Hackathon 48 Jam Data Terbuka 2017. Kedua-dua pertandingan ini diadakan secara serentak.

Selain daripada Pasukan daripada Bahagian Pengurusan Maklumat (MOTHACK), terdapat 2 lagi pasukan dari Jabatan Laut (MarineHack) dan MIROS (ROSHACK) turut mengambil bahagian.

Tahniah dan Syabas juga kepada MIROS telah diumumkan di tempat ke- 3 dalam kategori Sektor Awam Hackathon 48 jam Data Terbuka 2017.

Manakala Jabatan Laut Malaysia telah dimumkan di tempat ke 5 dalam kategori Sektor Awam Hackathon 48 Jam Data Terbuka 2017 dan Saguhati bagi kategori 24 jam Hackathon Mudah Alih 2017.

Program Hackathon ini bertujuan untuk menyediakan ruang perkongsian ilmu ke arah meningkatkan kualiti perkhidmatan digital, mempromosikan produk dan inisiatif digital perkhidmatan awam, menguji bakat dan kreativiti berdasarkan kemampuan masing-masing dari awal sehingga terciptanya satu produk inovatif yang tidak terikat kepada sebarang Hak Milik Intelektual serta menggalakkan penglibatan komuniti dalam membangunkan produk inovasi menggunakan Data Terbuka Sektor Awam.

Pasukan MOTHACK membawa pulang trofi, wang bernilai RM 3000.00 dan Sijil Penghargaan.

KEMENTERIAN PENGANGKUTAN MALAYSIA

Buletin ICT MOT

BIL. 3/2017 (Disember)

www.mot.gov.my

Bahasa Inggeris	Bahasa Melayu
fault tolerance	toleransi kesalahan
fingerprint reader	pembaca cap jari
digital imaging	pengimejan digital
significant digit	digit bererti
hacking	penggodaman
computer fraud	penipuan komputer
honeypot	komputer madu
information filtering	penapisan maklumat
data theft	pencurian data
transaction tracking	penjejakan urus niaga

Layari www.prpm.dbp.gov.my untuk rujukan atau semakan Bahasa Melayu atau
muat turun aplikasi mudah alih 'Carian Istilah' dari Galeri Aplikasi Mudah Alih Kerajaan Malaysia (GAMMA).

KEMENTERIAN PENGANGKUTAN MALAYSIA

Buletin ICT MOT

BIL. 3/2017 (Disember) www.mot.gov.my

ISTILAH ICT

BIL. 14/2017

MAMPU, JPM

NEGARAKU SEHATISEJIWA

bilik sembang / bilik bual	*chat room*
hantaran	*posting*
kumpulan berita	*newsgroup*
sumber khalayak	*crowd sourcing*
swafoto	*selfie*
swafoto berkumpulan	*groufie*
swafoto bersama	*wefie*
tanda pagar	*hashtag*
tunafoto	*photobomb*
tular	*viral*

SUMBER: Pusat Rujukan Persuratan Melayu (http://prpm.dbp.gov.my/)

Muat turun aplikasi mudah alih '**Carian Istilah**' dari Galeri Aplikasi Mudah Alih Kerajaan Malaysia (GAMMA)

KEMENTERIAN PENGANGKUTAN MALAYSIA

Buletin ICT MOT

BIL. 3/2017 (Disember) www.mot.gov.my

ISTILAH ICT

BIL. 15/2017

MAMPU, JPM

NEGARAKU

dalam talian	*online*
digitunai	*digicash*
kuki	*cookie*
longgok	*dump*
luar talian	*offline*
nyahpepijat	*debug*
papan kekunci	*keyboard*
pendigitalan	*digitalization*
rekayasa semula	*reengineering*
sohor kini	*trending*

SUMBER: Pusat Rujukan Persuratan Melayu (http://prpm.dbp.gov.my)

Muat turun aplikasi mudah alih '**Carian Istilah**' dari Galeri Aplikasi Mudah Alih Kerajaan Malaysia (GAMMA)

KEMENTERIAN PENGANGKUTAN MALAYSIA

Buletin ICT MOT

BIL. 3/2017 (Disember) www.mot.gov.my

ISTILAH ICT

BIL. 16/2017

MAMPU, JPM **NEGARAKU**

jeda	*pause*
keutuhan data	*data integrity*
log keluar	*log out/log off*
log masuk	*log in/log on*
mesej gesaan	*prompting message*
muat naik	*upload*
pad kekunci	*keypad*
pautan putus	*broken link*
pengguna istimewa	*privileged user*
tusuk	*poke*

SUMBER: Pusat Rujukan Persuratan Melayu (http://prpm.dbp.gov.my)

Muat turun aplikasi mudah alih '**Carian Istilah**' dari Galeri Aplikasi Mudah Alih Kerajaan Malaysia (GAMMA)

BULAN BAHASA KEBANGSAAN 2017 – Bahasa Jiwa Bangsa

KEMENTERIAN PENGANGKUTAN MALAYSIA

Buletin ICT MOT

BIL. 3/2017 (Disember)

www.mot.gov.my

ISTILAH ICT

BIL. 17/2017

MAMPU, JPM

akuan		*acknowledge*
butir data		*data item*
pakej sepadu		*integrated package*
penghantaran digital		*digital transmission*
pensirnaan		*zapping*
saling kendali		*interoperability*
sarat maklumat		*information overload*
seni bina terbuka		*open architecture*
sumber data		*data source*
talian maklumat		*infoline*

SUMBER: Pusat Rujukan Persuratan Melayu (http://prpm.dbp.gov.my)

Muat turun aplikasi mudah alih '**Carian Istilah**' dari Galeri Aplikasi Mudah Alih Kerajaan Malaysia (GAMMA)

BULAN BAHASA KEBANGSAAN

BULAN BAHASA KEBANGSAAN 2017 – Bahasa Jiwa Bangsa

KEMENTERIAN PENGANGKUTAN MALAYSIA

Buletin ICT MOT

BIL. 3/2017 (Disember)

www.mot.gov.my

ISTILAH ICT

BIL. 18/2017

MAMPU, JPM

aplikasi amali	*hands-on-application*
didik hibur	*edutainment*
e-panggilan	*e-hailing*
kad penyesuai	*adapter card*
mel remeh	*junk mail*
paut naik	*uplink*
pelayan awanama	*anonymous server*
penstriman langsung	*live streaming*
perayauan global	*global roaming*
skrin pipih	*flat screen*

SUMBER: Pusat Rujukan Persuratan Melayu (http://prpm.dbp.gov.my)

Muat turun aplikasi mudah alih '**Carian Istilah**' dari Galeri Aplikasi Mudah Alih Kerajaan Malaysia (GAMMA)

BULAN BAHASA KEBANGSAAN

BULAN BAHASA KEBANGSAAN 2017 – Bahasa Jiwa Bangsa

KEMENTERIAN PENGANGKUTAN MALAYSIA

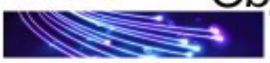
Buletin ICT MOT

BIL. 3/2017 (Disember) www.mot.gov.my

ISTILAH ICT

BIL. 19/2017

MAMPU, JPM

butang tekan		*push button*
emotikon		*emoticon*
Gbps (gigabit per saat)		*Gbps (gigabit per second)*
jadual carian		*look up table*
kameravideo		*videocam*
kawasan khas		*hotspot*
pengarkiban		*archiving*
pengkomputeran awan		*cloud computing*
tapak panas		*hot site*
tera air		*watermark*

SUMBER: Pusat Rujukan Persuratan Melayu (http://prpm.dbp.gov.my)

Muat turun aplikasi mudah alih '**Carian Istilah**' dari Galeri Aplikasi Mudah Alih Kerajaan Malaysia (GAMMA)