



MAJLIS KESELAMATAN NEGARA



#CaknaSiber



# LANGKAH MUDAH

## KESEDARAN KESELAMATAN SIBER

**NACSA**  
NATIONAL CYBER SECURITY AGENCY

**RAKAN STRATEGIK**



KEMENTERIAN KOMUNIKASI DAN  
MULTIMEDIA MALAYSIA



KEMENTERIAN SAINS,  
TEKNOLOGI DAN INOVASI



PELABAT KETUA PEGAWAI KESELAMATAN  
KERAJAAN MALAYSIA



UNIT PERENCANAAN STRATEGIK DAN  
PERENCANAAN KEMAMPUAN



**CyberSecurity**  
MALAYSIA

An agency under MOSTI



# 10 LANGKAH MUDAH KESEDARAN KESELAMATAN SIBER

---



1. GUNAKAN **KATA LALUAN**



2. **KEMASKINI** PERISIAN KESELAMATAN



3. **SIMPAN** DAN **LINDUNGI** MAKLUMAT



4. **ELAK** TERPEDAYA



5. **BERETIKA** MENGGUNAKAN  
INTERNET DAN MEDIA SOSIAL



6. **WASPADA** JENAYAH SIBER



7. **FIKIR** SEBELUM KLIK



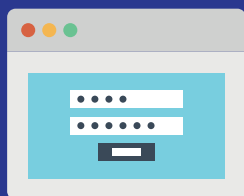
8. **LAPORKAN**



9. **AMBIL TAHU**



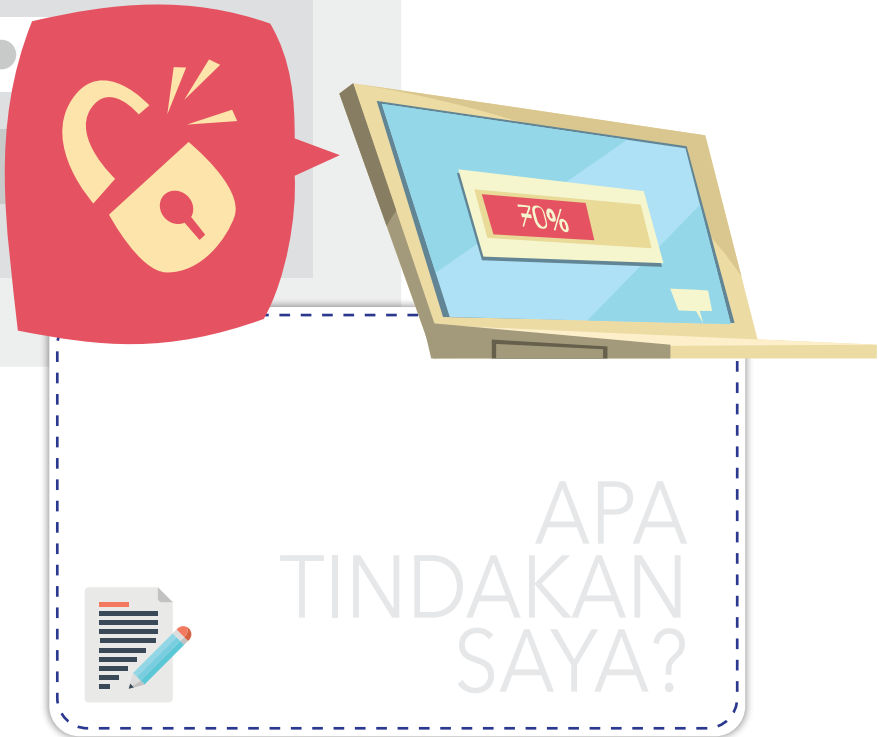
10. **PATUHI**



# GUNAKAN KATA LALUAN

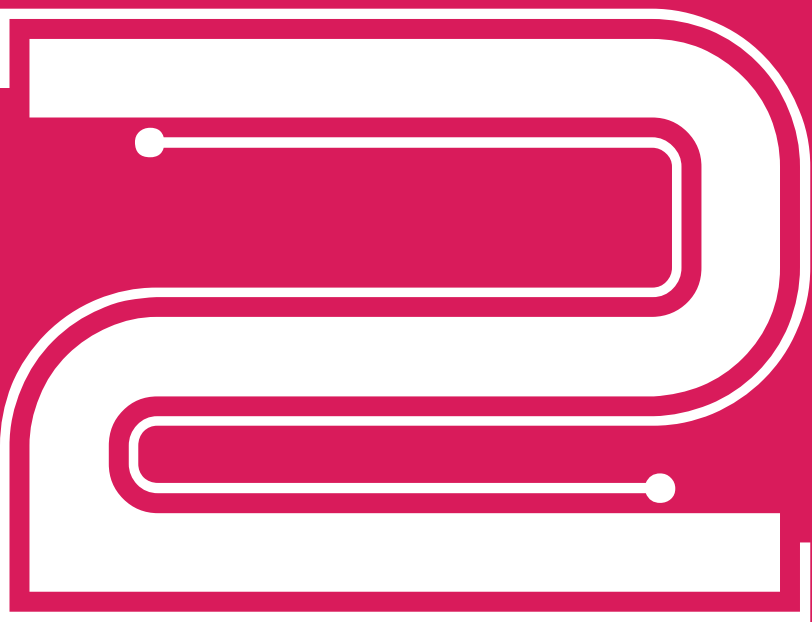


- ✓ Gunakan kata laluan yang kreatif (gabungan huruf, nombor dan simbol).
- ✓ Elakkan daripada mendedahkan kata laluan kepada orang lain.
- ✓ Sentiasa tukar kata laluan secara berkala dan elakkan daripada menggunakan kata laluan yang sama (berulang).
- ✓ Sulitkan (encrypt) penghantaran dokumen rasmi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





# KEMASKINI PERISIAN KESELAMATAN

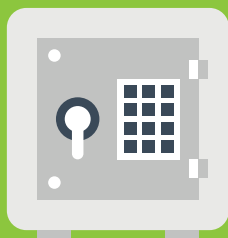


- ✓ Lengkapkan komputer dan gajet dengan perisian keselamatan (seperti anti-virus dan anti-spyware) terkini.
- ✓ Elakkan daripada menggunakan perisian keselamatan yang telah tamat tempoh.
- ✓ Gunakan perisian tulen.

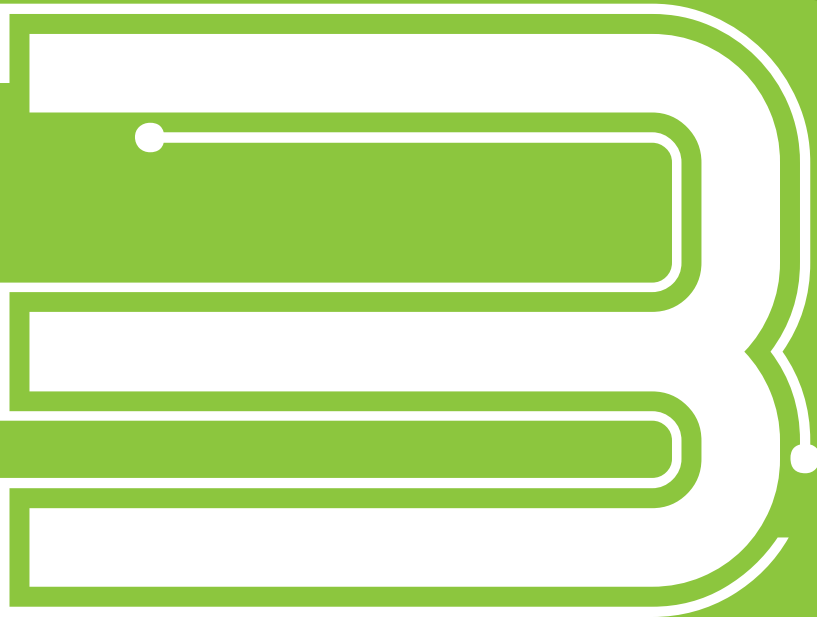


APA  
TINDAKAN  
SAYA?



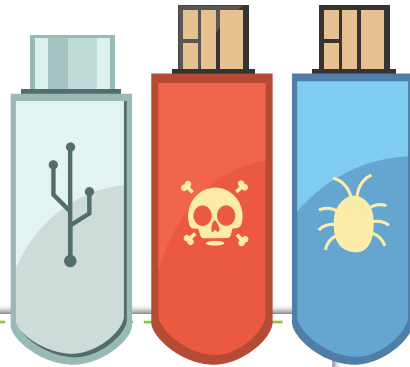


# SIMPAN DAN LINDUNGI MAKLUMAT





- ✓ Elakkan daripada memuat naik dokumen rasmi Kerajaan dalam *public cloud*.
- ✓ Sentiasa imbas peranti storan sebelum menggunakannya.
- ✓ 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 menggunakannya lagi.
- ✓ Pastikan meja kerja dikemas dan semua maklumat rasmi (termasuk yang berada di dalam peranti storan) disimpan di tempat yang selamat dan berkunci.



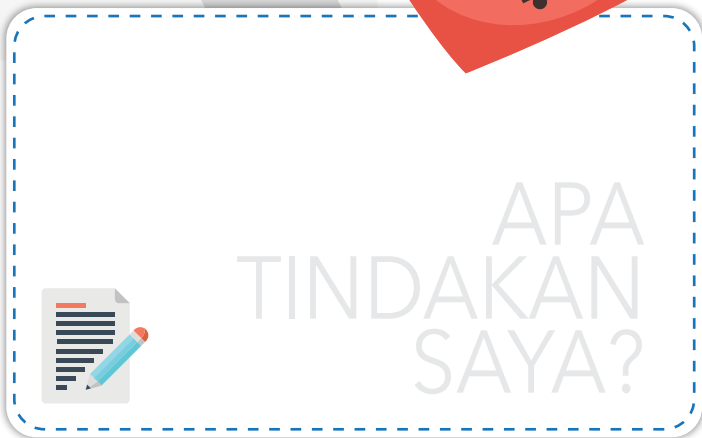
APA  
TINDAKAN  
SAYA?

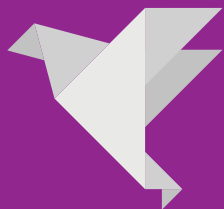


# ELAK TERPEDAYA



- ✓ 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.

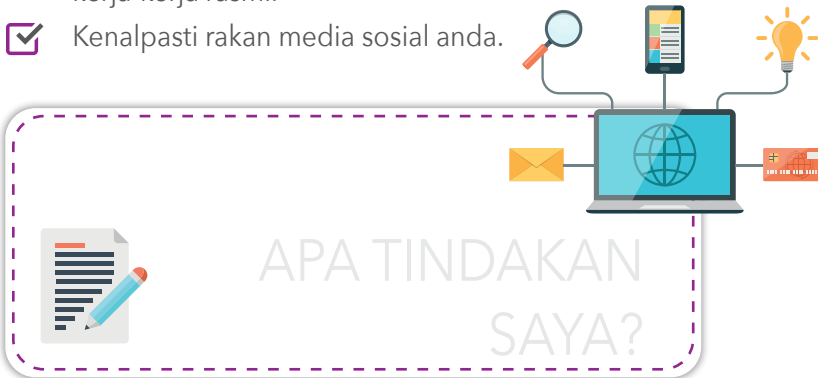




# **BERETIKA** MENGUNAKAN INTERNET DAN MEDIA SOSIAL



- ✓ 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 keselamatannya.
- ✓ 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 keselamatannya untuk melaksanakan kerja-kerja rasmi.
- ✓ Kenalpasti rakan media sosial anda.

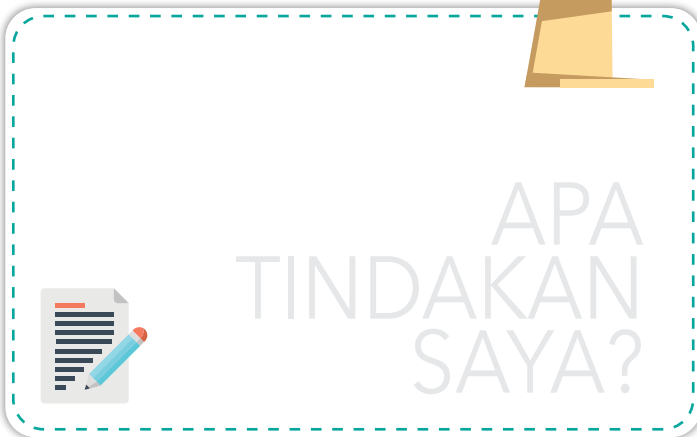




# WASPADA JENAYAH SIBER



- ✓ 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.





# FIKIR SEBELUM KLIK



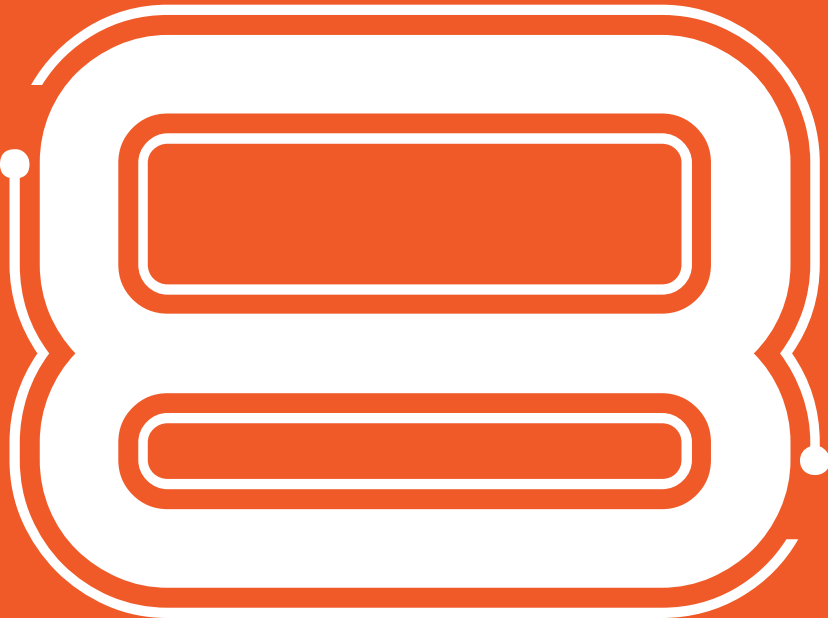


- ☑ Jangan klik pada e-mel, pautan atau lampiran yang mencurigakan (termasuk dari orang yang tidak dikenali). Padamkan e-mel tersebut.



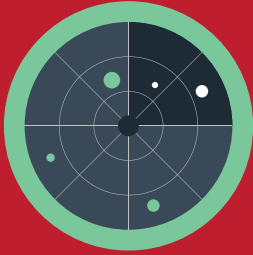


# LAPORKAN

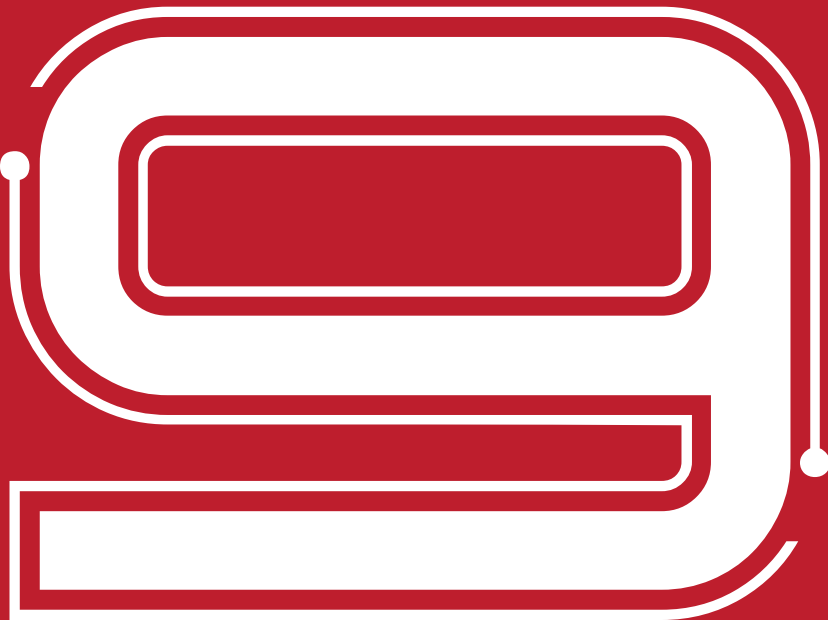


- Laporkan sebarang insiden kebocoran maklumat kepada pihak berkaitan.
- Laporkan dengan segera kehilangan sebarang aset ICT kerajaan (seperti peranti storan, komputer riba, komputer).
- Laporkan e-mel atau pautan yang mencurigakan atau dari orang yang tidak dikenali kepada Bahagian Teknologi Maklumat.
- Laporkan kepada pihak berkuasa sekiranya berlaku sebarang insiden jenayah siber seperti penipuan Internet.





# AMBIL TAHU

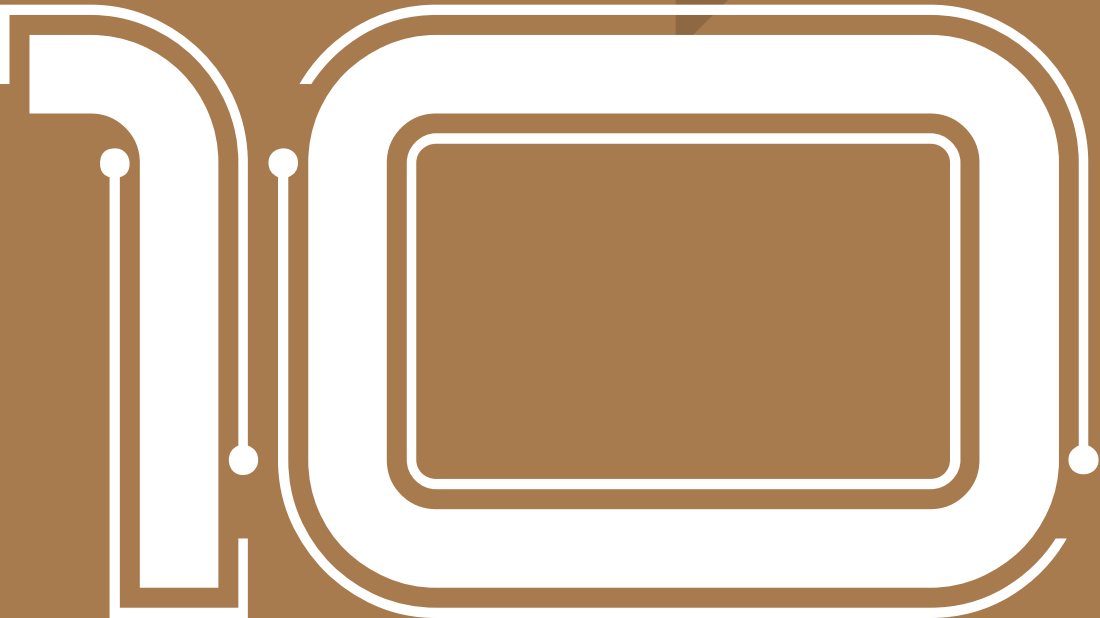


- ✓ Peka dengan trend ancaman siber terkini.
- ✓ Peka, fahami dan waspada mengenai kesan-kesan negatif akibat penyalahgunaan Internet.





# PATUHI



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



## Nota

A series of horizontal dashed lines for writing notes.



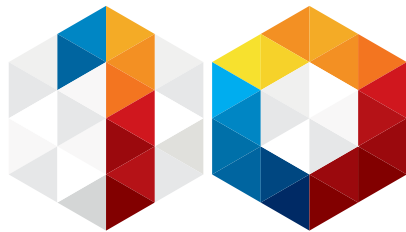


## Nota

A series of horizontal dashed lines for taking notes.



OKTOBER 2017



**BULAN KESEDARAN  
KESELAMATAN SIBER**