Berwaspada dengan keselamatan maklumat dan nikmatilah keseronokan menggunakan internet.

SKMM MCMC

Oficial Portal of
SURUHANJAYA KOMUNIKASI DAN MULTIMEDIA MALAYSIA
MALAYSIAN COMMUNICATIONS AND MULTIMEDIA COMMISSION

http://www.skmm.gov.my/

ASEAN · JAPAN
Information Security Awareness

Peka, Selamat dan Waspada

# Keselamatan Maklumat

Guna Internet Dengan Yakin

# Keselamatan Telefon Pintar

Telefon pintar telah menjadi sangat popular dan ini terbukti dengan peningkatan kadar penjualannya di seluruh dunia.

Telefon pintar adalah peranti komunikasi yang canggih berbanding telefon bimbit tradisional. Peranti ini membolehkan kita untuk melihat laman sesawang yang direka untuk platform PC dan pelbagai jenis aplikasi yang boleh dimuat turun secara percuma.

Versi terkini Sistem Pengoperasian (OS)*1 dan aplikasi*2 pada telefon pintar kerap dikemaskini*3. Ianya akan menambah baik fungsi telefon pintar dan seterusnya meningkatkan fungsi keselamatan.

*1 - OS adalah singkatan kepada sistem operasi yang merupakan perisian yang mengawal PC atau telefon pintar. Sebagai contoh di dalam Komputer Peribadi (PC), OS menguruskan pelbagai jenis fungsi-fungsi seperti I / O (Input / Output) yang mengawal input daripada papan kekunci, output untuk paparan, atau pencetak.

*2 - Application is s software for the specific purpose, such as word processing, or making spreadsheets. Users can choose appricatios they need, and use them after buliding them in the OS which has fundamental functions commonly used by every software.

*3 - Kemas kini bermakna pindaan kecil perisian untuk membetulkan bug, atau menawarkan penambahbaikan. Dengan menggunakan fungsi ini, pengguna boleh sentiasa mengemas kini aplikasi yang di pasang dengan versi terkini. Ia juga penting untuk mengemas kini perisian keselamatan untuk menjamin keselamatan maklumat.

## Risiko dan Ancaman

1 Bilangan malware yang menyasarkan telefon pintar semakin meningkat. Jika peranti anda dijangkiti oleh malware, maklumat peribadi seperti senarai nombor telefon dan maklumat peribadi lain mungkin dihantar ke pelayan luaran atau mungkin berlakunya transaksi caj yang tersembunyi.

2 Selain dijangkiti oleh malware, terdapat aplikasi yang dimuat turun akan menggunakan maklumat di dalam peranti atau meminta kandungan di dalam buku alamat untuk dihantar ke pelayan luaran. Sebagai contoh, terdapat aplikasi yang mendakwa direkabentuk untuk meningkatkan hayat bateri, tetapi sebenarnya ia menghantar maklumat buku alamat atau senarai nombor telefon terkandung di dalam peranti tersebut kepada pihak luar.

## Langkah Keselamatan

- Pastikan OS, aplikasi dan perisian anti-virus telefon pintar anda sentiasa dikemaskini dengan versi terkini. Ini adalah kerana telefon pintar mengandungi maklumat sensitif dan peribadi lain yang perlu dilindungi.
- Apabila memuat turun aplikasi, pastikan untuk memeriksa keaslian dan tahap kebolehpercayaan pihak yang membangunkan, menyedia dan membekalkan aplikasi tersebut. Pastikan anda menyemak terma dan syarat perkhidmatan berkenaan maklumat yang akan dikumpul dan bagaimana ia akan digunakan sebelum anda memberikan persetujuan untukmenggunakan aplikasi tersebut.





# Keselamatan Rangkaian Tanpa Wayar (Wireless LAN)

Sejak kebelakangan ini, PC telah menjadi lebih ringan dan kompak, serta penggunaan telefon pintar menjadi lebih popular. Tahap penggunaan Rangkaian Tanpa Wayar (Wireless LAN) yang meluas membolehkan pengguna mengakses internet dimana-mana sahaja samada di rumah mahupun pejabat.

Selain perkhidmatan berbayar yang disediakan oleh Penyedia Perkhidmatan Internet, penggunaan Wi-Fi awam secara percuma yang disediakan di lapangan terbang, stesen kereta api dan bangunan komersial juga turut meningkat.

## Risiko dan Ancaman

1 Memandangkan penggunaan Rangkaian Tanpa Wayar (Wireless LAN) yang meluas dan terbuka, capaian komunikasi tersebut berisiko terdedah kepada pintasan oleh pihak yang berniat jahat, melainkan langkah-langkah keselamatan dan pencegahan telah diambil oleh pengguna.
Selain itu, pencerobohan terhadap Rangkaian Tanpa Wayar (Wireless LAN) mungkin menyebabkan kebocoran maklumat peribadi atau rahsia syarikat, dan ianya berpotensi digunakan sebagai landasan untuk serangan ke atas sistem rangkaian/komputer lain.

2 Apabila menggunakan perkhidmatan Wi-Fi awam, PC atau telefon pintar anda mungkin disambung ke Rangkaian Tanpa Wayar (Wireless LAN) yang palsu. Sekiranya ini berlaku, sesi capaian dan komunikasi anda bermungkinan besar sedang diperhatikan.

## Langkah Keselamatan

- Pastikan tetapan keselamatan capaian router Wi-Fi anda ditetapkan kepada tetapan seperti WPA2 (Wi-Fi Protected Area Access 2) dan sebagainya. Ini memastikan capaian komunikasi sukar untuk dipintas serta menghalang capaian yang tidak dibenarkan. Apabila menetapkan tetapan enkripsi secara manual, pastikan penggunaan aksara secara rawak dengan bilangan aksara yang bersesuaian.
- Apabila menggunakan perkhidmatan Wi-Fi awam, sila gunakan laman sesawang berformat SSL*4 (laman sesawang URL yang bermula daripada "https://") sahaja dan sila nyahaktifkan tetapan perkongsian fail di peranti anda sebelum menggunakan perkhidmatan Wi-Fi awam tersebut.

*4 - SSL adalah singkatan kepada Lapisan Soket Selamat (Socket Secure Layer) yang merupakan protokol untuk menyamarkan data yang dihantar di laman sesawang.

# Penipuan Satu-Klik


Penipuan satu-klik merujuk kepada penipuan yang melibatkan wang. Ianya memaparkan skrin untuk bayaran tertentu seperti yuran pendaftaran atau bayaran penggunaan perkhidmatan selepas imej atau video di klik pada laman sesawang berkenaan.

Terkini, terdapat penipuan satu-klik yang menggunakan aplikasi telefon pintar dan perkhidmatan media sosial seperti blog*1 / perkhidmatan rangkaian sosial*2.

Selain kes penipuan "satu-klik", skrin bil pembayaran hanya akan dipaparkan selepas beberapa pengesahan seperti pengesahan umur, dan lain-lain lagi. Terdapat beberapa kes lain, teknik yang digunakan lebih licik dan canggih, seperti skrin bil tidak hilang walaupun selepas plug kuasa peranti telah ditutup.

*1 - Blog adalah singkatan kepada blog sesawang iaitu satu perkhidmatan di mana pengguna boleh menulis pendapat atau tanggapan mereka seperti jurnal dan pengunjung bebas memberi komen kepada penulisan/kandungan yang dipaparkan.

*2 - SNS adalah singkatan Perkhidmatan Rangkaian Sosial yang menyediakan laman sesawang yang mempunyai banyak fungsi seperti album diari atau gambar kepada orang ramai, atau berinteraksi dengan pengguna-penguna lain.

## Risiko dan Ancaman

1. Klik pada imej atau video percuma juga boleh menyebabkan pengguna dicaj tanpa disedari atau pengguna di halakan ke laman sesawang palsu/penipuan yang lain.

2. Terdapat beberapa kes di mana alamat IP*3 dan / atau maklumat pembekal disenaraikan pada skrin bil untuk menimbulkan rasa takut dan ianya kelihatan seperti individu itu telah dikenal pasti.

*3 - Alamat protokol internet adalah nombor pengenalan yang diberikan secara automatik kepada alat atau komputer apabila mereka disambungkan ke internet.

## Langkah Keselamatan

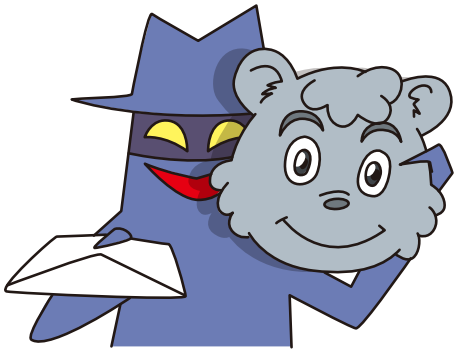
- Halang percubaan untuk capaian ke laman sesawang palsu/penipuan dengan menggunakan perisian penapisan atau lain-lain perisian keselamatan terkini. Juga pastikan hanya memuat turun aplikasi telefon pintar hanya dari laman sesawang penyedia aplikasi/perkhidmatan yang boleh dipercayai.
- Berhati-hati apabila menggunakan PC dan peranti pintar, penipuan satu-klik tidak dapat mengenal pasti anda, jadi jangan bertindak balas kepada cubaan untuk sebarang pembayaran. Untuk telefon pintar, berhati-hati terhadap sebarang aplikasi kerana maklumat yang disimpan pada peranti seperti maklumat peribadi dan maklumat sensitif lain mungkin didedahkan.
- Jika anda terjumpa salah satu daripada laman-laman sebegini, atau caj yang tidak diketahui dalam bil atau jika anda menerima perintah mahkamah, sila rujuk dan berunding dengan pihak berkuasa (kaunseling pentadbiran atau perundingan peguam percuma, dan lain-lain) untuk mendapatkan nasihat.





# Serangan E-mel Sasaran

Serangan e-mel sasaran adalah serangan yang disamarkan seolah-olah dihantar dari seorang kenalan pengguna, e-mel ini mungkin akan mengandungi lampiran berbahaya yang apabila diakses akan menjangkiti sistem dengan virus atau trojan.



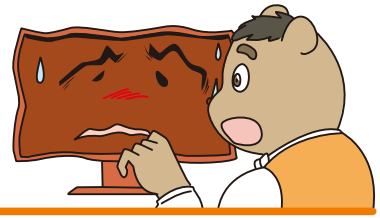
Satu contoh sasaran yang biasa disasarkan ialah sebuah organisasi atau pengguna individu. E-mel dengan lampiran yang dijangkiti virus dihantar dari penyerang yang berpura-pura mempunyai kaitan/hubungan dengan pihak tertentu atau rakan sekerja organisasi.

Terdapat kes-kes yang telah dilaporkan adalah berkaitan dengan kata laluan yang dicuri atau jangkitan virus, dan lain-lain lagi yang berpunca dari serangan e-mel yang disasarkan.

## Risiko dan Ancaman

1. Dalam kes serangan terkini, kaedah yang digunakan adalah dengan menyamar sebagai e-mel dari personaliti/organisasi yang boleh dipercayai oleh mangsa. Nama jabatan dan / atau individu yang benar-benar wujud digunakan, di samping menggunakan kandungan atau maklumat sulit yang hanya pihak-pihak tertentu yang mengetahui.

2. Jika virus disertakan dengan emel, membuka lampiran akan menyebabkan sambungan automatik ke pelayan luaran dan maklumat dalam komputer akan disalin dan dibocorkan.



## Langkah Keselamatan

- Jangan buka sebarang lampiran e-mel atau klik URL yang mencurigakan.
- Jika anda perlu atau terpaksa membuka e-mel yang mencurigakan, jangan panik dan jangan mematikan peranti. Putuskan sambungan rangkaian dan minta bantuan daripada pentadbir sistem.
- Pasang perisian antivirus dan pastikan ia sentiasa dikemaskini dengan versi terbaru.
- Pastikan semua aplikasi sentiasa dikemaskini secara berkala.

# Serangan DDoS

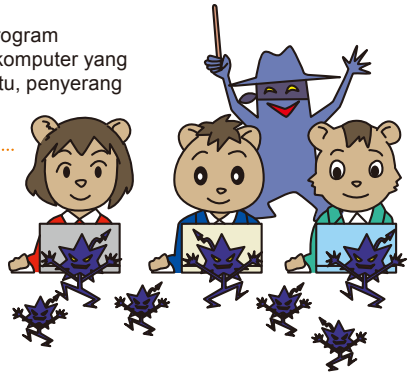
Serangan DDoS adalah serangan yang memfokuskan terhadap sesuatu pelayan komputer khusus, dengan menghantar sejumlah paket di dalam bilangan banyak/besar daripada komputer yang telah dicerobohi dari pelbagai rangkaian, sehingga sistem capaian dan komunikasi pelayan komputer yang disasarkan tidak mampu berfungsi seperi biasa.

DDoS: Distributed Denial of Service

## Risiko dan Ancaman

1. Penyerang akan menyamar serta memasang program berbahaya untuk melakukan serangan kepada komputer yang bukan sasaran akhir (pelayan komputer). Oleh itu, penyerang boleh menyerang mesin lain tanpa dikesan.

2. Komputer yang telah dicerobohi berupaya melakukan serangan-serangan lain seperti menjangkiti komputer lain dengan virus, menghantar e-mel spam atau menceroboh laman sesawang bagi pihak penyerang.



## Langkah Keselamatan

- Pastikan OS komputer, telefon pintar atau apa-apa peranti lain yang disambung ke internet dikemaskini dengan versi yang terkini.
- Pasang perisian antivirus dan pastikan bahawa ia adalah versi yang terkini.
- Pastikan semua aplikasi tambahan kepada OS sentiasa dikemaskini secara berkala.





# Etika Menggunakan Internet

Peningkatan penggunaan perkhidmatan rangkaian sosial telah menimbulkan pelbagai isu yang sebelum ini tidak dijangka.

Terdapat kes-kes yang melibatkan kandungan di internet di mana individu atau syarikat yang telah difitnah terpaksa mengeluarkan permohonan maaf secara umum.

## Risiko dan Ancaman

1. Besar kemungkinan juga terdapat paparan kandungan yang diposkan pada perkhidmatan rangkaian sosial boleh mendedahkan maklumat peribadi atau memfitnah orang lain iaitu melanggar kerahsiaan peribadi.

2. Paparan kandungan sebegini boleh menyebabkan pesalah membayar ganti rugi, teguran atau boleh ditahan oleh pihak berkuasa.

## Langkah Keselamatan

- Berhati-hati dengan tidak mendedahkan maklumat peribadi melalui perkhidmatan rangkaian sosial, blog, dan lain-lain. Paparan kandungan seperti artikel dan imej boleh mendedahkan maklumat lokasi semasa anda, jadi anda harus berhati-hati.
- Malah di internet, pastikan anda mempertimbangkan privasi dan maruah orang lain dan melakukan pemeriksaan kandungan sebelum memuatnaik kandungan dan maklumat ke rangkaian sosial.

# Penetapan, Pengurusan ID dan Kata Laluan yang wajar

Di dalam pengunaan e-mel, pembelian secara talian, perbankan internet dan perkhidmatan lain secara dalam talian, terdapat pelbagai kaedah pengesahan identiti/ kebolehpercayaan yang boleh digunakan dan yang paling popular adalah kombinasi ID / kata laluan.

Baru-baru ini terdapat peningkatan serangan siber yang menyasarkan pengguna bagi mendapatkan maklumat akaun seperti kata pengenalan pengguna (User ID) dan kata laluan.


## Risiko dan Ancaman

**1** Pihak ketiga mungkin menyamar sebagai pengguna sah dan mendedahkan maklumat atau menyebabkan kerugian kewangan jika ID / kata laluan adalah gabungan yang sangat mudah (seperti tarikh lahir 4 digit, atau "9999", dan lain-lain) atau jika ia tidak diuruskan dengan berhati-hati (sebagai contoh, kata laluan dibiarkan pada pada monitor, dan lain-lain).

**2** Jika menggunakan ID / kata laluan yang sama untuk pelbagai laman sesawang dan maklumat tersebut dibocorkan dari salah satu laman sesawang, besar kemungkinan capaian di laman sesawang yang lain juga akan berlaku.


## Langkah Keselamatan

- Tetapkan kata laluan dengan rentetan secara rawak dengan sekurang-kurangnya terdiri daripada 8 aksara yang mengandungi kombinasi nombor, huruf kecil dan besar dan simbol. Pastikan juga kata laluan kerap ditukar.
- Jangan berkongsi kata laluan dengan orang lain atau menggunakan kata laluan yang sama untuk laman sesawang yang berlainan. Jika sesebuah laman sesawang memaklumkan bahawa kata laluan anda bocor, tukar kata laluan anda bukan sahaja di laman sesawang tersebut, tetapi juga laman sesawang yang lain menggunakan kata laluan yang sama.
- Elakkan memasukkan maklumat peribadi ke dalam komputer yang digunakan oleh orang ramai seperti di kafe internet dan tempat-tempat awam yang lain.





# E-mel Spam 1

E-mel adalah medium komunikasi yang mudah untuk menghantar dan menerima mesej tanpa mengira jarak mereka. Walau bagaimanapun, dari sudut penerima, mungkin terdapat banyak e-mel yang tidak diperlukan, mesej spam, samada yang dihantar atau diterima.

Oleh kerana bilangan besar e-mel spam yang dihantar, terdapat isu-isu di mana peralatan di pihak penyedia perkhidmatan menjadi beban dan membawa kepada kelewatan untuk menerima / menghantar mesej.

## Risiko dan Ancaman

**1** Terdapat kes-kes di mana terdapat komputer yang akan menjana sejumlah besar alamat e-mel dan menghantar e-mel secara rawak ke senarai e-mel tersebut. Oleh itu, penggunaan alamat e-mel pendek dan nama-nama popular boleh mengakibatkan kemungkinan peningkatan penerimaan e-mel spam.

**2** Sebahagian daripada alamat e-mel sah yang digunakan untuk penghantaran e-mel spam dipungut melalui pendaftaran perkhidmatan palsu seperti pendaftaran penawaran perkhidmatan secara percuma atau melalui prosedur yang direka.
Selain itu, membuka fail yang dilampirkan menerusi e-mel atau mencapai pautan dalam URL e-mel boleh menghalakan kepada satu laman sesawang yang berbahaya / palsu atau dijangkiti virus.

## Langkah Keselamatan

- Alamat e-mel harus mengandungi sebilangan besar simbol dan nombor secara rawak supaya ia sukar untuk diteka.
- Berhati-hati memasukkan alamat e-mel anda ke laman sesawang atau menunjukkan alamat e-mel anda pada lama sesawang.
- Jika perlu untuk melayari laman sesawang yang mungkin tidak sepenuhnya boleh dipercayai, ia lebih berkesan untuk menggunakan alamat e-mel yang boleh didapati secara percuma berbanding dengan menggunakan e-mel yang dibekalkan oleh penyedia perkhidmatan.

# E-mel Spam 2

E-mel Spam bukan sahaja boleh menyebabkan ketidak selesaan kepada penerima atau mengganggu tugasan harian, tetapi dengan kaedah terkini yang semakin berbahaya dan bijak, ia boleh membawa pengguna ke laman sesawang yang berbahaya/palsu di mana wang anda mungkin dicuri, atau ianya berupaya melangkaui sistem penapis e-mel spam.

Telefon pintar boleh dijangkiti oleh virus yang terkandung di dalam e-mel spam, dimanipulasi untuk menghantar sejumlah besar e-mel spam tanpa pengetahuan pengguna.

## Risiko dan Ancaman

**1** Terdapat kes-kes di mana komputer akan menjana sejumlah besar alamat e-mel dan menghantar e-mel secara rawak. Oleh itu, penggunaan alamat e-mel pendek dan nama-nama popular boleh mengakibatkan kemungkinan peningkatan penerimaan e-mel spam.

**2** Sebahagian daripada alamat e-mel sah yang digunakan untuk penghantaran e-mel spam dipungut melalui pendaftaran perkhidmatan palsu secara percuma atau melalui prosedur yang direka. Selain itu, membuka fail yang dilampirkan kepada e-mel atau mengakses pautan dalam e-mel boleh menghalakan kepada satu laman sesawang yang tidak dibenarkan atau dijangkiti virus.

## Langkah Keselamatan

- Cuba sekat e-mel spam dengan menggunakan langkah balas keselamatan atau fungsi anti-spam yang disediakan oleh penyedia perkhidmatan internet atau perisian penapisan.
- Jika anda menerima e-mel spam, padam tanpa membukanya. Jangan buka lampiran atau mengakses pautan dari e-mel yang mencurigakan. Ia mungkin juga berkesan dengan memanjangkan e-mel spam kepada pembekal perkhidmatan atau agensi awam.
- Ambil langkah balas keselamatan pada telefon pintar dan juga pada PC.





# Lindungi telefon pintar dan komputer anda.

Telefon pintar dan komputer adalah peranti dan alat yang sungguh berguna, Namun, harus diingat bahawa peranti-peranti ini mudah terdedah kepada bahaya seperti dijangkiti virus. Sentiasa beringat untuk mematuhi tiga tip utama keselamatan maklumat untuk memastikan keselamatan apabila menggunakan komputer dan telefon pintar.

### Tiga panduan utama dalam memelihara keselamatan maklumat

**Kendalikan maklumat penting peribadi dengan baik.**

**Lindungi komputer anda dengan mengemaskini aplikasi keselamatan terkini.**

**Jangan akses laman sesawang yang mencurigakan atau mebuka e-mel yang tidak dikenali.**

Langkah-langkah keselamatan maklumat boleh disamakan dengan penggunaan tali pinggang keledar apabila kita menaiki kereta. Langkah keselamatan ini adalah sangat penting dan tidak boleh diabaikan apabila menggunakan telefon pintar atau komputer.