

CyberSAFE in Schools

Panduan Penggunaan
Internet Secara Selamat

Safer Internet For All

DiGi

Rakan Kerjasama:



CyberSecurity
MALAYSIA

An agency under MOSTI

Kandungan

2

Menjamin Keselamatan Peranti Digital Anda

6

Melindungi Penyambungan Anda

10

Etika Penggunaan Peranti Mudah Alih



Pengenalan

Hari ini, peranti mudah alih (termasuk telefon bimbit dan tablet) bukan sahaja digunakan untuk berhubung serta mengambil dan berkongsi gambar, ia juga digunakan untuk melayari internet, merakam video, mendengar muzik, dan bersosial dalam talian. Ia seakan-akan mempunyai komputer-mini di dalam poket atau di telapak tangan anda.

Evolusi teknologi yang pesat membolehkan kita mengakses internet di mana jua. Ia juga membolehkan kita menyimpan maklumat peribadi dan kerja di dalam peralatan mudah alih.

Walau bagaimanapun, jika anda kehilangan peranti mudah alih, anda akan menghadapi risiko lebih daripada sekadar kehilangan senarai kenalan. Anda juga akan kehilangan semua maklumat sensitif dan peribadi lain yang disimpan di dalamnya serta mendedahkan diri anda kepada risiko yang lebih besar.

Kami telah merekabentuk panduan ini untuk melengkapkan anda dengan maklumat yang akan membantu mengekal keselamatan dalam talian dan meningkatkan keselamatan alat peranti mudah alih anda. Di samping itu, ia juga dapat memberi panduan kepada anda dan menyokong penggunaan internet secara bertanggungjawab bersama rakan-rakan dan keluarga.



Menjamin Keselamatan Peranti Digital Anda

Anda perlu melihat peranti digital anda seperti barang berharga yang lain. Ini kerana peranti digital masa kini boleh menyimpan dan mempunyai pelbagai maklumat peribadi yang penting. Maka, kita harus menjamin keselamatan peranti digital serta isi kandungannya.

TAHUKAH ANDA

Kita lebih cenderung untuk kehilangan telefon bimbit sebanyak 15 kali berbanding dengan komputer riba, dan ini merupakan kerugian adalah ancaman terbesar pada pengguna peranti mudah alih.
(www.Mcafee.com)

Menjamin Keselamatan Peranti Digital Anda



INGAT

Peranti mudah alih
kini menyimpan
pelbagai maklumat.
**PASTIKAN IA
TERJAMIN SELAMAT!**

Menjamin keselamatan peranti mudah alih anda secara fizikal



Pastikan peranti mudah alih anda dikonfigurasi dengan *auto-lock* selepas beberapa saat. Biarpun dalam keadaan yang berkunci, elakkan ia daripada terbiar sendiri kerana ia senang dicuri atau tercicir.



Berhati-hati apabila menggunakan peranti mudah alih anda di tempat awam. Elakkan dari menggunakannya semasa berjalan, ataupun di kawasan yang padat dengan orang ramai.



Jika anda kehilangan peranti mudah alih anda yang mempunyai data dan terikat dengan operator telefon mudah alih, segera laporkan kehilangan tersebut kepada operator berkenaan. Ingat, anda bertanggungjawab ke atas setiap caj panggilan, teks dan penggunaan data sehingga talian anda disekat.

Memanfaatkan Ciri-Ciri Keselamatan Asal di dalam Peranti Mudah Alih

- 1** Kebanyakan peranti mudah alih mempunyai sistem sekuritinya tersendiri. Dengan menggodam atau mengubah ciri-ciri asal, ia akan melemahkan sistem yang tersedia ada.
- 2** Muat turun aplikasi daripada sumber yang boleh dipercayai sahaja. Sebelum memuat turun, selidik aplikasi tersebut dengan membaca ulasan pengguna dan penilaian. Jangan lupa, sentiasa kemaskini aplikasi anda.
- 3** Baca dasar privasi sebelum memasang apa-apa aplikasi pada peranti mudah alih anda. Pertimbangkan seberapa banyak maklumat peribadi anda yang diperlukan oleh aplikasi tersebut dan jika ia akan berkongsi maklumat itu dengan orang lain. Jika anda tidak pasti, jangan muat turun aplikasi tersebut.



TAHUKAH ANDA

Anda boleh menetapkan kata laluan pada aplikasi di dalam peranti mudah alih anda.

Tip pembinaan kata laluan:

- Bina kata laluan yang kompleks dengan menggunakan gabungan huruf kecil & besar, nombor dan simbol.
- Panjang katakunci adalah di antara 8- 14 karakter.
- Kata laluan tidak melibatkan nama anda, atau tarikh lahir, nombor telefon mahupun nama syarikat.

Melindungi Peranti iOS dan Android Anda

PERANTI iOS

Senarai Semak

o **Aktifkan kata laluan atau kod laluan**

Menetapkan kata laluan atau kod laluan adalah langkah pertama yang sangat bagus bagi menjaga keselamatan peranti iOS anda. Cara tetapan kod laluan adalah dengan Tap *Seting* -> *Umum* -> *Kunci Kod Laluan*

o **Pengaktifan Cari iPhone/cari iPad**

Sama ada hilang ataupun di curi, anda boleh meningkatkan peluang untuk mendapatkan kembali iPhone mahupun iPad anda dengan memuat turun aplikasi *Cari iPhone/Cari iPad*.



o

Tetapkan Pengehadan Anda

Apabila anda tetapkan pengehadan, anda akan menetapkan kod laluan yang akan menghadkan daripada servis tertentu ditukar oleh pencuri. Cara untuk menetapkan *Pengehadan* adalah dengan Tap *Seting* -> *Umum* -> *Pengehadan*, kemudian pilih servis yang mana anda ingin tetapkan pengehadan.

PERANTI ANDROID

19:35

• **Mencipta Corak, PIN, kata laluan ***

Untuk mengelakkan daripada peranti anda diceroboh oleh orang tanpa kebenaran, anda boleh tetapkan seting seperti berikut: *Aturan* -> tap *Sekuriti* -> skrin kunci dan pilih samada untuk menetapkan corak, PIN ataupun kata laluan.

• **Melabur dalam aplikasi keselamatan yang efektif**

Pertimbangkan untuk memasang aplikasi keselamatan yang efektif bagi menjaga keselamatan serta melindungi anda dari ancaman yang sedia ada dan terbaru. Jenama *Lookout* ataupun *Avast* adalah salah satu aplikasi keselamatan yang boleh dipertimbangkan.



• **Setup profil pengguna yang berbeza**

Jika anda selalu berkongsi peranti anda dengan orang lain, anda dinasihatkan agar membuat profil pengguna yang berbeza untuk setiap pengguna. Ini akan menghadkan daripada fail anda di akses oleh orang lain. Caranya adalah seperti berikut: *Aturan* -> tap *Pengguna* -> tambah pengguna.

** Langkah-langkah penetapan mungkin berbeza mengikut versi Android dan pembuat/pengilang peranti*



Melindungi Penyambungan Anda

Apabila menggunakan peranti mudah alih untuk menghantar dan menerima data atau melayari internet, ia adalah penting untuk menggunakan sambungan yang selamat. Ingat, bahawa seperti dalam dunia sebenar, anda juga akan menghadapi risiko keselamatan di dunia digital. Sambungan yang tidak selamat boleh mendedahkan anda kepada bahaya dalam talian.

INGAT

Sentiasa matikan WiFi (Wi-Fi, perkhidmatan lokasi dan Bluetooth) apabila tidak digunakan dan “disable” fungsi sambungan secara automatik pada peralatan mudah alih anda.

Melindungi Penyambungan Anda



INGAT

Pastikan anda sentiasa log keluar laman seperti emel, facebook, dan bukan hanya menutup pelayar. Ini kerana orang yang mendapat peralatan anda berpotensi untuk log masuk ke semua akaun anda. Jangan sekali-kali menyimpan kata laluan dan *username* di dalam peralatan mudah alih anda.

Jenis-jenis Penyambungan

Dalam dunia teknologi mobil masa kini, berikut adalah di antara pilihan penyambungan yang biasa ada pada kebanyakan peralatan mudah alih di pasaran:



Peralatan kepada Peralatan

- NFC (Near Field Communication) adalah teknologi RFID jarak dekat tanpa wayar yang menghubungkan aplikasi apabila peralatan mudah alih berada pada jarak yang sangat rapat (contoh: peranti Android)
- Bluetooth: teknologi tanpa wayar yang membolehkan komunikasi antara peralatan mudah alih yang mempunyai Bluetooth yang serasi. Ia digunakan untuk penyambungan jarak dekat di antara peralatan mudah alih (seperti komputer riba, telefon, PDA, kamera digital dll)



Data Rangkaian

- Ianya merujuk kepada pelan data mudah alih yang anda telah langgani pada peranti mudah alih anda



WiFi Awam

- Lebih dikenali sebagai Wifi Hotspot, ianya merujuk kepada akses tanpa wayar percuma atau secara berbayar di lokasi awam sebagaimana yang diperuntukkan oleh pemilik premis kepada pengunjung.

Berhati-hati apabila mengguna WiFi Awam



- **Tiada yang sulit pada WiFi Awam**

Jika anda melayari internet menggunakan sambungan yang tidak selamat (cth: WiFi Percuma di restoran makanan segera), anda akan terdedah kepada penjenayah siber yang boleh melihat dan mencuri maklumat anda.

- **Jangan mengirim atau menerima data yang sensitif melalui WiFi Awam**

Apabila melakukan transaksi sensitif (contohnya perbankan dalam talian), pastikan ia dilakukan pada rangkaian terjamin. Pertimbangkan penggunaan pelan data operator pengendali mudah alih anda kerana kebanyakan penyambungan peranti menyulitkan data yang di transaksi antara tiang sel dengan peranti mudah alih anda.

Berhati-hati apabila mengguna Bluetooth dan Geo-lokasi

- **Jadikan ia satu tabiat untuk menutup sambungan Bluetooth atau perkhidmatan lokasi apabila tidak digunakan**

Ini untuk mengelakkan peralatan mudah alih anda di ceroboh dan mengelakkan daripada orang asing mengetahui di mana anda berada. Anda dinasihatkan supaya tidak dedahkan nama sebenar anda di Bluetooth / tanpa wayar identiti.

- **Berfikir sebelum mengirim**

Geo-lokasi membolehkan orang ramai untuk mencari anda menggunakan GPS peranti mudah alih anda. Untuk keselamatan, hanya berkongsi lokasi anda dengan orang yang anda percayai.

- Apabila memuat naik gambar, berfikir dua kali sebelum anda Geotag gambar tersebut. Anda mungkin tidak mahu semua orang tahu di mana anda tinggal atau bersekolah.





Etika Penggunaan Peranti Mudah Alih

Ia bukan semata mata menerangkan cara menjaga peralatan mudah alih anda yang mempunyai info mengenai diri anda. Ia juga merangkumi tanggungjawab anda sebagai pengguna peralatan tersebut. Ini bermaksud, cara tingkah laku anda yang diterima oleh masyarakat dalam talian.

TAHUKAH ANDA

Kebanyakan orang terlalu mendedahkan maklumat mengenai diri mereka dalam talian.
(www.intel.com)

Etika Penggunaan Peranti Mudah Alih

Sensitif terhadap maklumat



Untuk Diri Anda – Jangan sesekali memberi maklumat peribadi seperti nama anda, alamat rumah & sekolah, nombor telefon, lokasi di mana anda berada, infomasi mengenai ibubapa anda, gambar, katakunci, maklumat MyKad anda tanpa kebenaran ibubapa anda.

Untuk Orang Lain – Anda harus menjaga infomasi orang lain, sebagaimana anda menjaga infomasi diri anda.

Berhati-hati dengan Pembuli - Siber



Untuk Diri Anda – Minta pertolongan dari adik-beradik atau ibubapa mahupun guru jika anda di buli dalam talian. Jangan takut.

Untuk Orang Lain – Berfikir sebelum anda menulis sesuatu yang tidak baik dalam talian. Jangan lakukan dalam talian, jika anda tidak akan lakukan di hadapan seseorang. Apabila kawan anda di buli dalam talian, nasihatkan meraka agar mendapat pertolongan dari orang yang lebih dewasa.



108 suka

lihat semua komen



Untuk Diri Anda – Satu gambar, seribu terjemahan. Ingat, apa yang anda maksudkan, tidak semestinya sama dengan apa yang difahami oleh orang lain. Maka berhati-hati apabila memuat naik gambar anda agar tidak terlalu mendedahkan infomasi mengenai diri anda.

Untuk Orang lain – Sebelum mengambil gambar atau memuat naik gambar yang melibatkan orang lain, pastikan anda meminta kebenaran terlebih dahulu. Terutama jika melibatkan kanak-kanak.



Suka



Komen



INGAT

Jika anda tidak boleh berkongsi sesuatu perkara yang baik, maka jangan berkongsi apapun.

Membuli di alam siber merupakan satu jenayah. Buli di siber adalah termasuk mesej gangguan di buat melalui sms dan kenyataan di dalam laman muka buku kepunyaan orang lain.

Ketagihan terhadap peralatan mudah alih

Untuk Diri Anda – Peralatan mudah alih merupakan alat yang sangat bagus jika digunakan secara sederhana. Jangan abaikan mereka di sekeliling anda. Penggunaan peralatan mudah alih semasa memandu dan melintas jalan adalah sangat merbahaya. Tidak kurang juga ia mengganggu kesihatan seperti kekurangan tidur akibat asyik menggunakan peralatan ini.

Untuk Orang lain – Ramai akan menganggap anda adalah seorang anti-sosial kerana terlalu taksu dengan peralatan mudah alih anda sehinggalah tidak mempedulikan orang di sekeliling anda. Hormati undang-undang yang melibatkan penggunaan peralatan mudah alih.

Untuk maklumat lanjut

www.digi.com.my/digicybersafe

Merupakan satu program kesedaran keselamatan siber oleh CyberSecurity Malaysia, sebuah agensi di bawah kawalselia Kementerian Sains, Teknologi dan Inovasi, dengan tujuan menyebarkan kesedaran mengenai penggunaan internet dengan selamat. Untuk maklumat lanjut, sila layari www.cybersafe.my

CyberSecurity
MALAYSIA

CyberSAFE
Cyber Security Awareness For Everyone

Cyber999 merupakan pusat bantuan insiden keselamatan siber. Untuk membuat laporan, sila email cyber999@cybersecurity.my atau telefon **1-300-88-2999 / 60192665850**.

Cyber999

Talian 24 jam khas untuk mangsa kanak-kanak penderaan, keganasan rumah tangga dan bencana alam.

TALIAN NUR
15999

Merupakan talian bantuan 24 jam untuk kanak-kanak. Jika anak anda perlu bercakap dengan seseorang, hanya perlu memanggil talian 15999 atau layari facebook.com/childline15999 untuk berhubung meminta bantuan.

15999
Childline
Ready to Help



CyberSAFE in Schools

Panduan Penggunaan
Internet Secara Selamat

Safer Internet For All



DiGi

Disahkan oleh:

