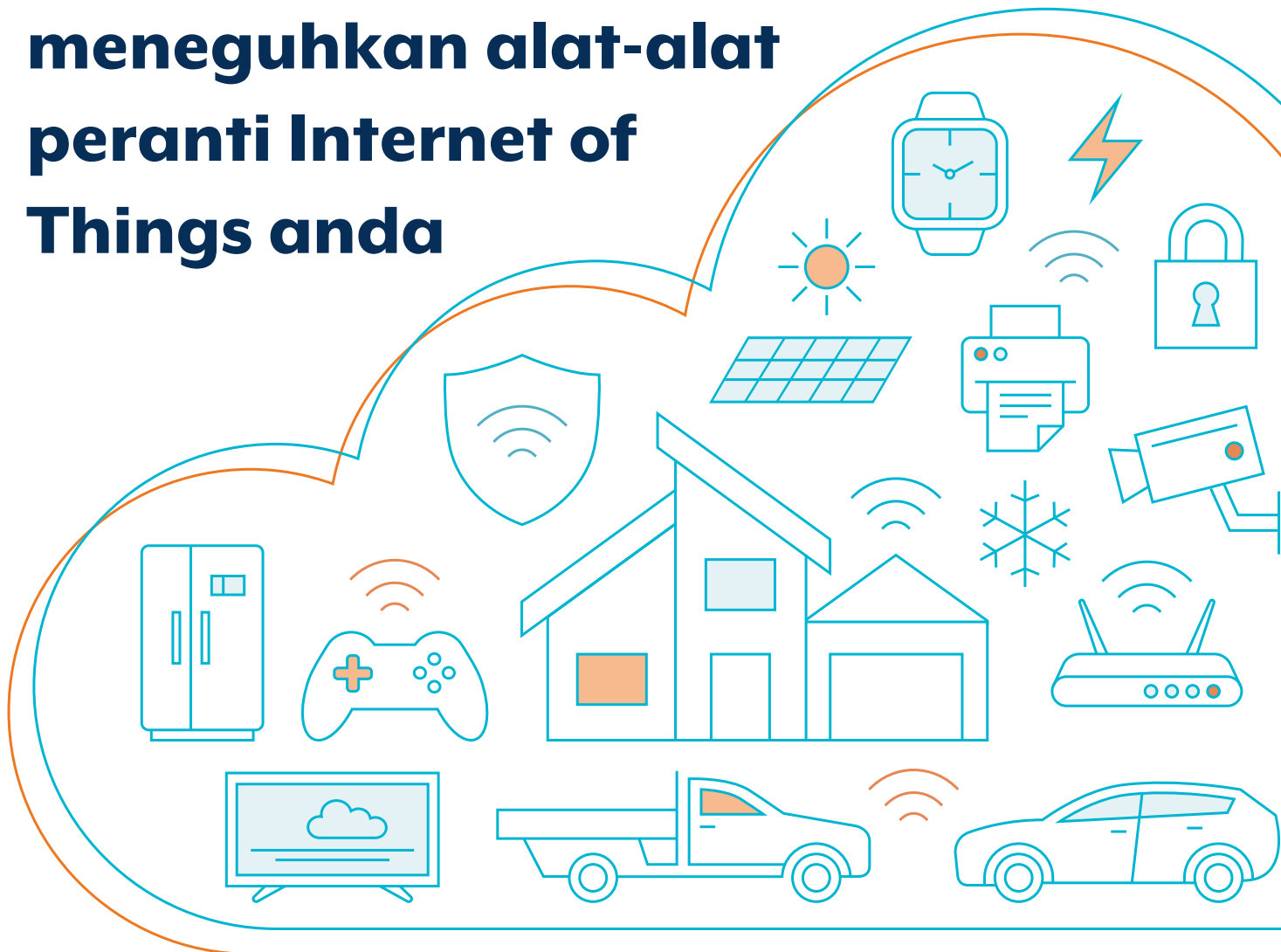




Petua untuk meneguhkan alat-alat peranti Internet of Things anda



Pusat Keselamatan Siber Australia (The Australian Cyber Security Centre) telah membangunkan maklumat ini untuk menolong pihak masyarakat membeli dan menggunakan alat-alat peranti Internet of Things (IoT) secara teguh. Alat peranti IoT ialah sebuah barangan harian yang ditambah dengan keterhubungan kepada internet. Contoh-contoh alat peranti IoT termasuk pemantau bayi, dron, kamera keselamatan, televisyen pintar dan panel solar. Alat-alat peranti di dalam rumah dan perniagaan amnya menggunakan Wi-Fi atau jaringan selular, misalnya 4G atau 5G, untuk berhubung kepada internet.

Kebanyakan alat peranti IoT yang biasanya ditemui di dalam rumah dan perniagaan di Australia tidak direka dengan mengambil kira soal keselamatan. Hal ini telah mengakibatkan kerentanan pada alat-alat peranti ini untuk dikompromi menerusi internet. Insiden-insiden seperti ini boleh membenarkan penjenayah siber akses tidak diminta ke alat peranti dan data peribadi anda bagi tujuan berniat jahat.



Sebelum membeli sebuah alat peranti IoT

la penting untuk menyelidik sesebuah alat peranti sebelum membelinya, kerana para pengeluar masing-masing menyampaikan tahap keselamatan yang berbeza. Sebelum membeli sesebuah alat peranti, bandingkan alat peranti serupa yang dijual oleh pengeluar lain. Perkara-perkara untuk dipertimbangkan termasuk:

-  **1. Adakah alat peranti itu dibuat oleh sebuah syarikat yang dikenali dan boleh dipercayai dan dijual oleh sebuah kedai yang dikenali dan boleh dipercayai?** Syarikat-syarikat yang dikenali dan boleh dipercayai lebih boleh diyakini untuk mengeluarkan alat peranti yang mempertimbangkan soal keselamatan. Kedai-kedai yang dikenali dan boleh dipercayai lebih boleh diyakini untuk hanya menjual alat-alat peranti daripada syarikat yang boleh diyakini, dan mempunyai rantaian-bekalan lebih ketat, yang memastikan alat peranti itu sampai ke tangan anda sebagaimana yang diingini pihak pengeluarnya.
-  **2. Adakah kata laluan anda boleh ditukar?** Adalah baik untuk menukar kata laluan anda. Namun begitu, jika alat peranti itu dikirim dengan kata laluan lalai yang lemah, hal ini menjadi satu perkara yang lebih mustahak. Sesebuah alat peranti dengan keselamatan baik sepatutnya mempunyai kata-kata laluan yang unik, tidak boleh diramal, kompleks dan sukar untuk diteka, kerana kata laluan lalai yang lemah menyampaikan cara paling mudah untuk menyerang sesebuah alat peranti.
-  **3. Adakah pihak pengeluar menyampaikan pengemaskinian?** Ia penting bagi syarikat untuk menawarkan pengemaskinian untuk memperbaiki kerentanan alat peranti apabila ia ditemui. Contohnya, jika perisian pada sesebuah alat peranti mengandungi kerentanan yang diketahui atau penggadam membangunkan cara baharu untuk mengkompromikan alat peranti anda, pengemaskinian adalah diperlukan untuk menyampaikan pembaikan.
-  **4. Data apa yang akan dipungut alat peranti itu dan data itu akan dikongsi dengan siapa?** Maklumat mengenai data apa yang akan dipungut dan bagaimana ia akan diguna sepatutnya disediakan secara terus pada laman web pengeluar atau di dalam dasar privasi mereka. Ia penting untuk sentiasa mempertimbangkan maklumat yang dipungut oleh aplikasi dalam talian atau boleh ubah tersebut.
-  **5. Adakah alat peranti itu hanya akan melakukan apa yang anda mahu ia lakukan?** Membeli sebuah alat peranti yang melakukan lebih daripada apa yang ada perlu, termasuk menghubungkannya kepada internet, mungkin akan mengurangkan keselamatan anda. Keupayaan alat peranti itu yang anda tidak akan guna boleh meningkatkan kerentanan alat peranti itu kepada serangan tanpa menyampaikankan sebarang manfaat kepada anda.

Alat Peranti IoT

Pertimbangkan beberapa soalan ringkas sewaktu anda memasang alat peranti anda, untuk membantu anda memastikan jaringan dan data anda lebih terjaga.

-  **1. Adakah alat peranti itu perlu dihubungkan kepada internet?** Kerana ia boleh dihubungkan kepada internet tidak bererti ia patut berbuat demikian. Alat-alat peranti yang tidak dihubungkan kepada internet kurang berkemungkinan untuk dikompromi. Jika anda tidak akan menggunakan ciri-ciri yang memerlukan keterhubungan kepada internet, anda sepatutnya menimbang sama ada ia perlu dihubungkan kepadanya atau tidak.
-  **2. Adakah alat peranti itu berada di dalam sebuah lokasi yang teguh?** Jika alat peranti itu tidak perlu dipasang di dalam sebuah kawasan tidak teguh, memasangkannya di dalam sebuah lokasi teguh boleh mengurangkan risiko pengkompromian fizikal.
-  **3. Adakah saya perlu menukar nama pengguna dan kata laluan lalainya?** Ia penting bagi anda untuk menggunakan kata laluan atau frasa laluan yang kuat. Jika alat peranti anda tidak dikirim dengan kata laluan yang unik, tidak boleh diramal, kompleks dan sukar untuk diteka, kata laluan ini perlu ditukar. Nama pengguna dan kata laluan lalai akan dipungut dan dihantar dalam talian, yang akan merentankan alat peranti anda.
-  **4. Adakah jaringan Wi-Fi saya dipasang dengan teguh, dan adakah ia mempunyai kata laluan yang teguh?** Teguhkan jaringan Wi-Fi dan router anda untuk menjadikannya lebih sukar bagi para penyerang untuk mengakses alat peranti anda dan jaringan anda.

Langkau langkah seterusnya

Pasangkan sebuah jaringan Wi-Fi tambahan pada router anda untuk alat-alat peranti IoT sahaja. Ia boleh dikenali pada router Wi-Fi anda sebagai jaringan 'tetamu' ('guest'). Jika alat peranti IoT anda tidak perlu berkomunikasi antara satu sama lain, upayakan ciri 'pemencilan pelanggan' ('client isolation'). Memastikan alat-alat peranti IoT anda dipencilkan daripada data sensitif anda memastikan bahawa sebuah pengkompromian sesebuah alat peranti IoT tidak akan memberikan akses kepada alat peranti atau data anda yang lain.

-  **5. Adakah ciri-ciri alat peranti yang tidak perlu sudah dimatikan?** Jika alat peranti anda mempunyai ciri-ciri yang tidak dikehendaki atau tidak diperlukan (misalnya kamera atau mikrofon), ia sepatutnya dinyahupayakan sejauh mana yang boleh.

Langkau langkah seterusnya

Cari pengesetan pengkonfigurasi yang menyebut mengenai mengupayakan akses jarak jauh kepada pengantaramuka pentadbiran web alat peranti itu daripada LAN lokal atau WAN/ internet. Pastikan ia diset kepada LAN lokal, kecuali jika anda sendiri memerlukan akses jarak jauh.

Menyelenggarakan sebuah alat peranti IoT

Terdapat beberapa perkara penting untuk diingat selepas alat peranti IoT anda telah dipasang dan digunakan. Ia termasuk:

-  **1. Boot kembali alat-alat peranti anda dengan kerap.** Virus-virus mungkin hadir jika alat peranti IoT itu menjadi semakin perlahan atau tidak boleh dioperasi. Kebanyakan malware disimpan dalam memori dan boleh dikeluarkan dengan mudah daripada sebuah pembootan kembali sesebuah alat peranti, iaitu, dengan mematikan dan menghidupkan semula alat peranti itu. Jika alat peranti itu terus beroperasi dengan perlahan atau tidak boleh dioperasikan selepas pembootan kembali dilakukan, cuba sebuah pengesetan kilang, tetapi anda perlu sedar bahawa kaedah ini mungkin akan memadamkan semua data pengguna dan pengesetan peribadi anda.
-  **2. Terapkan pengemaskinian dengan kerap.** Sesetengah alat peranti menerapkan pengemaskinian secara automatik. Bagi alat peranti yang tidak, semak dengan pengeluaranya secara kerap dan terapkan pengemaskinian apabila ia disediakan. Apabila pengemaskinian tidak lagi disediakan bagi alat peranti anda, pertimbangkan untuk menaiktaraf ke sebuah alat peranti lebih baharu di mana pengemaskinian disediakan. Alat peranti yang tidak mempunyai akses kepada pengemaskinian keselamatan tidak akan dilindungi jika kerentanan baharu ditemui, dan alat-alat peranti ini mungkin akan menjadi satu risiko kepada jaringan anda, privasi anda dan data anda.
-  **3. Matikan alat peranti anda bila ia tidak digunakan.** Meninggalkan alat peranti yang tidak diguna dan tidak dipantau tetap dipasang dan dihubungkan kepada jaringan Wi-Fi anda bagi tempoh masa yang berlanjutan boleh meningkatkan kemungkinan alat-alat peranti anda diserang. Satu pilihan untuk mencapai hal ini secara automatik ialah dengan menggunakan sebuah penentu masa punca kuasa hanya untuk menyampaikan kuasa kepada alat peranti itu semasa waktu-waktu yang tertentu.
-  **4. Awasi kenaikan signifikan dalam penggunaan internet bulanan atau bil anda.** Kenaikan signifikan dalam penggunaan internet atau caj-caj bil boleh menunjukkan bahawa alat peranti anda telah dikompromi. Kecuali jika hal ini akan disiasat oleh sesebuah jabatan IT di dalam perniagaan anda, sebuah pengesetan kembali kilang patut diterapkan (namun begitu anda patut sedar bahawa kaedah ini mungkin akan memadamkan semua data pengguna dan pengesetan peribadi anda), diikuti penukaran kata laluan anda.

Melupuskan sebuah alat peranti IoT

Melupuskan sebuah alat peranti (dengan membuang atau menjualkannya) mungkin akan memberi orang lain akses mudah kepada maklumat atau data peribadi anda.

Cara-cara untuk mengelakkan hal ini daripada berlaku termasuk:

-  **1. Memadamkan semua data dan maklumat peribadi.** Pengeluar patut menyediakan satu kaedah cara bagaimana untuk memadamkan data dan maklumat peribadi anda daripada kedua-dua alat peranti dan aplikasi-aplikasi yang berkaitan dengannya. Memadamkan maklumat peribadi anda memastikan tiada sesiapa yang akan memperoleh akses kepadanya selepas anda telah melupuskan alat peranti itu. Padamkan akaun dalam talian anda jika ia tidak lagi diperlukan tanpa alat peranti IoT itu.
-  **2. Lakukan pengesetan kembali kilang bagi alat peranti itu.** Sebuah pengesetan kembali kilang direka untuk memadamkan data yang disimpan dalam simpanan lokal dan mengeset kembali kata-kata laluan, nama-nama pengguna dan pengesetan kembali kepada keadaan lalainya. Semak buku panduan alat peranti itu atau laman web pengeluaranya untuk maklumat tentang cara bagaimana untuk melakukan satu pengesetan kembali kilang.
-  **3. Putuskan kaitan alat peranti itu daripada telefon-telefon bimbit dan alat-alat peranti lain.** Melupuskan sebuah alat peranti yang masih mempunyai akses kepada alat-alat peranti lain, jaringan atau akaun-akaun dalam talian anda menyampaikan potensi kepada pihak lain untuk mendapatkan akses. Pastikan anda memeriksa alat-alat peranti lain anda dan buang mana-mana pasangan yang ia ada dengan alat peranti yang anda ingin lupuskan. Buang sebarang kebenaran yang diberi kepada aplikasi boleh alih yang tidak lagi diperlukan.
-  **4. Buang sebarang media yang boleh ditanggalkan (misalnya pemacu kilat USB, kad memori dsb) yang dipasang kepada alat peranti itu.** Media yang boleh ditanggalkan mungkin mengandungi data peribadi yang tidak dipadamkan di dalam sebuah pengesetan kilang dan patut dikeluarkan secara fizikal, dibinasakan secara fizikal dan dilupuskan secara berasingan daripada alat peranti itu.



Bantuan

Hubungi The Australian Signals Directorate's Australian Cyber Security Centre (Pusat Keselamatan Siber Australia Direktorat Semboyan Australia) dengan menghantarkan e-mel kepada asd.assist@defence.gov.au atau sila panggil Talian Panas 24/7 untuk mendapatkan bantuan mustahak pada **1300 CYBER1 (1300 292 371)**.

Laporkan jenayah siber kepada ReportCyber di www.cyber.gov.au/report

Hubungi IDCARE menerusi laman web mereka www.idcare.org jika anda telah mengalami kecurian identiti.

Sila layari www.cyber.gov.au untuk nasihat bagi anda dan keluarga anda. Sign up for the free ACSC Alert Service on recent online threats.

Mari jadikan Australia tempat paling selamat untuk berhubung dalam talian.

Untuk nasihat keselamatan siber, sila layari www.cyber.gov.au

Penafian

Bahan di dalam panduan ini adalah bersifat umum dan tidak harus dianggap sebagai nasihat perundangan atau digantung sebagai bantuan dalam apa-apa keadaan atau kecemasan tertentu. Dalam sebarang hal mustahak, anda harus mendapatkan nasihat profesional bebas tentang apa yang anda sedang alami sendiri.

Pihak Komanwel tidak menerima tanggungjawab atau tanggungan ke atas sebarang kerosakan, kerugian atau perbelanjaan yang ditanggung akibat daripada pergantungan kepada maklumat yang terkandung dalam panduan ini.

Hakcipta Terpelihara

© Komanwel Australia 2025

Dengan pengecualian Jata Negara dan di mana ia dinyatakan sebaliknya, semua material yang disampaikan dalam penerbitan ini telah disediakan di bawah sebuah [Creative Commons Attribution 4.0 International licence | creativecommons.org](https://creativecommons.org/licenses/by/4.0/).

Untuk mengelakkan sebarang keraguan, ini bererti bahawa lesen ini hanya bertakluk ke atas bahan-bahan yang disampaikan di dalam dokumen ini.



Butir-butir syarat-syarat berkenaan lesen ini boleh diperolehi dari laman web Creative Commons website kerana ia merupakan [Kod Undang-Undang bagi lesen CC BY 4.0 | creativecommons.org](https://creativecommons.org/licenses/by/4.0/).

Penggunaan Jata Negara

Terma-terma di bawah mana Jata Negara boleh diguna telah diperincikan dalam laman web Department of the Prime Minister and Cabinet [Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au](https://pmc.gov.au/commonwealth-coat-of-arms-information-and-guidelines).

Untuk maklumat lanjut, atau untuk melaporkan sebuah kejadian keselamatan siber, sila hubungi kami:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Nombor ini tersedia untuk digunakan di dalam Australia sahaja.

