

## **MELINDUNGI KOMPUTER DARI PENGGODAM DAN VIRUS**

Anda boleh melindungi komputer, data yang sensitif dan rangkaian internet di rumah daripada penggodam dan virus dengan mengambil beberapa langkah asas. Jika anda menyambung kepada internet menerusi rangkaian jalur lebar (Streamyx atau Jaring), anda perlu mengambil perhatian yang lebih terhadap keselamatan komputer dan mengambil langkah-langkah tambahan.

Menggunakan internet melalui rangkaian jalur lebar dari rumah dapat meningkatkan lagi tahap keserenokkan dalam melayari internet. Tetapi pengguna internet jalur lebar harus mengambil langkah-langkah tambahan untuk melindungi komputer dan fail-fail di dalamnya. Dengan kelajuan pemindahan data yang berkelajuan tinggi dari dan ke komputer anda, di tambah pula dengan masa komputer dihubungkan ke internet dengan lebih lama, menyebabkan ia lebih menjadi sasaran penggodam berbanding pengguna 'dial-up'. Dengan mengambil beberapa langkah asas pencegahan dengan menggunakan alat-alat yang sesuai, anda boleh memainkan perana dalam melindungi alam siber dari ancaman penggodam. Pada masa yang sama juga, ada akan melindungi komputer dan maklumat anda daripada kecurian, disalah-guna atau dimusnahkan.

**1. Selalu Menggunakan Perisian Anti-Virus** – Dan selalulah memastikan perisian anda dikemaskini. Lebih 500 jenis virus ditemui setiap bulan. Anda tidak hanya melindungi diri anda, tetapi juga mereka yang berhubung dengan anda melalui internet. Senarai perisian anti-virus percuma ada disertakan di dalam CD Ipositif.

Virus komputer ialah perisian yang boleh merebak dengan menjangkiti fail-fail 'executable' atau fail sistem di dalam cakera keras atau cakera liut dengan menggandakan diri mereka. Virus biasanya merebak tanpa pengetahuan atau kehendak pengguna komputer sendiri. Virus boleh menyebabkan kehilangan data dan memerlukan kos yang tinggi untuk membaikinya. Virus juga boleh merebak dari satu komputer ke komputer-komputer yang lain.

Anda boleh mengurangkan risiko virus dengan memasang dan menggunakan perisian anti-virus. Perisian anti-virus boleh mengimbas dan mengesan komputer anda dan email-email yang diterima daripada virus dan kemudiannya membuang virus berkenaan. Banyak virus baru ditemui setiap hari. Untuk memastikan perisian anda menawarkan tahap perlindungan yang tinggi, anda perlu mengemaskinikan perisian anti-virus anda dengan kerap. Kebanyakan perisian anti-virus mengandungi ciri-ciri yang membolehkan anda memuat-turun fail-fail kemaskini yang berkenaan secara automatik apabila anda dihubungkan ke internet.

**2. Selalu Menggunakan 'Firewall'** – 'Firewall' ialah 'kunci dalaman' untuk maklumat di dalam komputer anda. Kebanyakan sistem operasi komputer yang terbaru telahpun mengandungi perisian 'firewall'; anda hanya perlu mengaktifkannya. Terdapat banyak perisian 'Firewall' yang boleh dimuat turun atau dibeli untuk melindungi komputer anda. Senarai 'Firewall' percuma disertakan di dalam CD Ipositif.

'Firewall' ialah perisian atau perkakasan yang menghalang data yang tidak dikenali atau tidak diluluskan dari memasuki atau keluar dari komputer anda. 'Firewall' membantu anda menjadi lebih selamat di internet dan menghalang anda dari

berkomunikasi dengan sumber-sumber yang tidak diketahui. Untuk mendapatkan perlindungan optimum, anda perlu menggunakan kedua-dua perisian anti-virus dan juga 'firewall'.

**3. Belajar risiko dan peraturan mengenai perkongsian maklumat dan sambungan internet –** Anda boleh didedahkan kepada bahaya melalui e-mail, perkongsian fail, sambungan jalur-lebar dan sambungan 'Wi-Fi'.

### **3.1 Perkongsian-Fail:**

Apabila berkongsi fail melalui rangkaian rakan-ke-rakan (peer-to-peer), pastikan anda mengetahui segala peraturan dan tips untuk memastikan apa yang anda kongsi sah di sisi undang-undang dan selamat. Perisian perkongsian fail juga dinamakan perisian rakan-ke-rakan. Daripada kesemua jenis perisian-perisian ini, yang paling bahaya ialah 'Napster' dan perisian yang hampir sama dengannya (sila lihat senarai di bawah). Perisian perkongsian fail berfungsi dengan menjadikan fail-fail komputer anda boleh dimuat turun terus ke komputer yang lain dengan menggunakan perisian yang sama. Biasanya ia digunakan untuk berkongsi muzik, video dan fail-fail perisian; biasanya ia menyalahi undang-undang perlindungan harta intelek. Tidak dinafikan bahawa teknologi perkongsian rakan-ke-rakan mempunyai banyak faedah jika digunakan secara betul dan sah, tetapi malangnya ia digunakan secara meluas hari ini untuk berkongsi fail-fail muzik secara tidak sah dengan orang ramai.

Berikut ialah senarai perisian perkongsian yang popular. Anda mungkin mahu melihat sama ada fail ini dipasang di komputer anda:

Sistem Operasi Windows: Aimster , Audio Galaxy, Bearshare , Gnutella , Gnucleus, Grokster, iMesh, KaZaa, Limewire, Morpheus, SwapNut , WinMX

Sistem Operasi Mac: Aimster , Limewire , Mactella

### **3.2 Sambungan Wi-Fi:**

Jika anda menggunakan internet tanpa-wayar, anda harus memastikan langkah-langkah tambahan diambil untuk melindungi komputer dan rakaian komputer anda.

#### **Keselamatan Wi-Fi**

Semakin ramai pengguna internet menggunakan rakaian Wi-Fi untuk membuat sambungan tanpa wayar ke internet. Teknologi baru dan menarik ini kini banyak digunakan di rangkaian rumah dan bistro. Melayari internet secara tanpa-wayar mencetus kebimbangan baru mengenai keselamatan komputer. Jika anda mengguna rangkaian Wi-Fi di rumah, anda perlu mengambil langkah-langkah tambahan untuk memastikan komputer anda selamat. Kebanyak orang memilih untuk membiarkan sambungan rangkaian Wi-Fi mereka terbuka dan ini mencipta 'hot-spot' yang membolehkan sesiapa sahaja yang berdekatan kawasan itu untuk membuat sambungan ke internet. Anda harus memahami risiko sebelum membuka

rangkaian Wi-Fi anda kepada umum. Berikut ialah tips mengenai keselamatan Wi-Fi:

### ***Ketahui Risiko dan Berhati-Hati Sebelum Membuka Rangkaian Wi-Fi kepada Umum***

- [Adakah 'Hot-Spot' Anda Menyalahi Peraturan Pembekal Servis Internet \(TMNet / Jaring\) Anda?](#) Sesetengah pembekal internet jalur-lebar melarang pengguna berkongsi sambungan Wi-Fi dengan orang yang tidak dikenali. Larangan ini biasanya terkandung dalam syarat-syarat perkhidmatan oleh pembekal internet semasa anda mendaftar untuk menggunakan internet.
- [Adakan komputer dan rangkaian anda selamat? Pastikan kata laluan komputer anda sukar diteka dan dihafal.](#) Ini amat penting terutamanya jika anda mempunyai rangkaian komputer di rumah. Semestinya anda tidak mahu orang yang tidak dikenali menggunakan sambungan Wi-Fi anda untuk mengakses komputer anda.
- [Adakah anda telah menukar kata-laluan stesen utama \(base station\)?](#) Kebanyakan stesen utama Wi-Fi menggunakan kata-laluan yang senang diteka seperti 'admin' atau 'default' – membolehkan penggodam untuk mengambil alih aturan stesen utama anda. Pastikan anda menukar kata-laluan stesen utama Wi-Fi kepada yang sukar diteka tetapi mudah diingati.

### ***Tips untuk menutup rangkaian Wi-Fi dari orang yang tidak dikenali***

Jika anda mahu melindungi rangkaian Wi-Fi dari orang yang tidak dikenali, terdapat beberapa langkah yang boleh diambil:

- [Jangan siarkan SSID anda.](#) Ini merupakan langkah yang paling mudah untuk mencegah seseorang dari memasuki rangkaian Wi-Fi anda – bagaimanapun ia masih belum lagi selamat. Secara automatik, semua stesen utama Wi-Fi menghebahkan kehadiran mereka – menggunakan pengenalan yang dipanggil 'Service Set Identifier (SSID)' kepada sesiapa yang berdekatan.
- ['Encrypt' kata laluan rangkaian wireless anda](#)
- [Pastikan stesen utama hanya menerima alamat 'MAC' anda](#)

### ***Tips Untuk Mengantar Maklumat Sensitif Melalui Rangkaian Wi-Fi***

- [Jangan hantar fail yang sensitive jika anda tahu rangkaian Wi-Fi tidak selamat](#)
- [Gunakan 'Virtual Private Network \(VPN\)' untuk memastikan keselatan maklumat yang dihantar melalui Wi-Fi](#)

### **3.3 E-mail:**

Kebanyakan virus merebak melauai email. Apabila virus menjangkiti komputer anda, ia akan menggandakan diri dengan merebak kepada nama-nama yang terdapat pada buku alamat email. Untuk mencegah dari email yang tidak diinginkan, gunakan penapis email

**4. Putuskan sambungan ke internet jika tidak aktif** – Jika anda tidak gunakan sambungan internet, tutupkan sambungan. Tiada siapa yang dapat menyerang

komputer anda jika ia tidak disambungkan ke internet. Ini bertambah penting untuk sambungan jalur lebar

**5. Gunakan kata laluan yang unik** – Jangan kongsi kata laluan anda dengan rakan-rakan.

**6. Sentiasa mengawal perisian anda** - Perisian dan sistem operasi dilengkapi dengan ciri-ciri keselamatan yang kadang kala tidak digunakan. Belajar cara-cara untuk mengemaskinikan sistem operasi secara automatik, mengaktifkan 'firewall' atau tidak mengaktifkan sebarang fungsi-fungsi yang boleh membahayakan komputer.

**7. Guna Alatan yang bersesuaian untuk melindungi komputer anda** – belajar menggunakan alatan yang bersesuaian untuk melindungi komputer anda dari penggodam dan virus.

#### ***'Firewalls'***

Lindungi dari penggodam dengan mengaktifkan 'firewall' yang sudah tersedia atau muat turun 'firewall' jika ia tidak disediakan oleh sistem operasi anda. Perisian 'firewall' membolehkan anda melayari internet dan memuat turun bahan-bahan yang anda mahu tanpa gangguan dari penggodam atau virus. Perisian 'firewall' percuma ada disertakan pada CD IPositif ini

#### ***Perisian Antivirus***

Perisian anti-virus jika selalu dikemas kini dapat menghalang hampir semua virus yang boleh membahayakan komputer anda. Kebanyakan perisian anti-virus boleh dimuat turun dari internet. Perisian anti-virus percuma ada disertakan pada CD IPositif ini

#### ***Penapis E-mail***

Kebanyakan virus merebak melalui email. Untuk mengurangkan jumlah email yang tidak dikehendaki, gunakan penapis email. Kebanyakan perisian email dilengkapi dengan penapis email yang tersedia.

**8. Ambil Tindakan Secepat Mungkin** – Jika anda merasakan komputer anda telah digodam atau dijangkiti virus, hubungi pembekal internet anda (TMNet atau Jaring)

**Putuskan sambungan internet apabila dijangkiti virus atau digodam:** Anda boleh melakukannya dengan mencabut sambungan telefon atau kabel ke di computer anda. Gunakan komputer yang tidak dijangkiti untuk memuat turun perisian virus yang terkini. Sentiasa mengemas kini perisian anti-virus dan 'firewall' untuk mencegah dari segala bahaya dan ancaman.

**Laporkan Pencerobahan, Penggodaman dan Virus yang Serius:** Apabila anda mengambil langkah untuk membersihkan virus atau penggodam, laporkan insiden yang serius kepada pembekal servis internet anda. Lampirkan juga maklumat

Ipositif: Melindungi Komputer dari Penggodam dan Virus

terperinci yang diperolehi dari perisian anti-virus atau 'firewall' semasa virus atau penggodam menyerang semasa membuat laporan.

Compiled by: Ezmir Mr ([ezmir@mmu.edu.my](mailto:ezmir@mmu.edu.my)) with referenced to <http://www.getnetwise.org/>