

## Informasi Cara Kerja Hacker

Apakah ada hal yang mustahil untuk dilakukan oleh seorang Hacker? Setiap hari kita membaca berita tentang hacker yang membobol rekening secara online, menyerang jaringan bisnis, mencuri identitas pengguna jejaring sosial dan hal lain yang dapat mendatangkan kerugian pada masyarakat. Sehingga sudah sewajarnya kalau kita harus lebih waspada dengan pengamanan internet yang kita gunakan setiap hari.

Kenyataannya bahwa kebanyakan **cara kerja hacker** menggunakan [trik](#) yang sama untuk masuk ke komputer dan mencuri informasi berharga yang kita miliki. Dari keterangan berikut ini diharapkan Anda untuk lebih waspada agar dapat terlindungi dari jari pintar si hacker.

### Secara Online

Beberapa [cara kerja hacker](#) atau jalan yang digunakan seorang hacker secara online adalah:

- 1. Spam:** Sebagian besar [cara kerja hacker](#) atau *serangan hacker* dimulai dengan junk mail alias spam. Hacker akan mengirimkan pesan dengan judul yang menggoda seperti "I love You" atau "Free Gift!" atau "You are Winner". Untuk ratusan atau bahkan ribuan alamat email yang diperoleh secara ilegal. Email spam ini dapat menipu Anda agar memberikan informasi yang bersifat pribadi, mengajak Anda berkunjung ke situs berbahaya/porno, atau bahkan memberikan link untuk men-download program menarik yang sebenarnya program tersebut akan memberikan total kontrol si hacker atas komputer Anda! Hacker sangat pintar dalam pengetahuan komputer mereka, dan akan berusaha keras untuk membuat email spam dengan kata-kata yang sangat meyakinkan.
- 2. Download:** Men-download file dari Internet menjadi sangat populer sejak Napster diperkenalkan ke dunia maya. Dan sekarang, meski telah ada peraturan hukum yang melarang pembajakan software, musik dan film, tetapi dengan cepat melalui mesin pencari Google kita akan sangat mudah menemukan jutaan website yang didedikasikan untuk men-download musik, video, software dan gambar (baik secara legal maupun ilegal) dari Internet. Tetapi hati-hati, ketika Anda men-download file tersebut bisa saja Anda akan mendapatkan "bonus" di balik file yang Anda dapatkan, yaitu berupa spyware, adware bahkan virus yang bersembunyi bersama file tersebut.
- 3. Popup:** Semua orang tahu bahwa popup itu menjengkelkan, tapi apakah Anda tahu bahwa popup juga membawa resiko keamanan pada komputer? Popup adalah salah satu jalan yang digunakan hacker sebagai cara untuk mendapatkan perhatian Anda dan menipu Anda agar melakukan hal-hal yang bisa memasukkan informasi pribadi Anda. Anda mungkin sering ketika membuka sebuah website dan tiba-tiba ada jendela baru yang otomatis terbuka, sebaiknya langsung di close saja popup tersebut. Hacker menggunakan ini untuk mengiklankan produk dan jasa yang tampaknya sah, namun di dalam popup ini tersembunyi virus atau spyware yang dapat mengintai ketika Anda meng-klik-nya.
- 4. ActiveX:** teknologi ActiveX sering digunakan oleh banyak situs web terkenal seperti bank dan toko online untuk membuat transaksi online Anda lebih baik dan cepat. Sayangnya, hacker telah menemukan cara untuk mengeksploitasi ActiveX dan menggunakannya untuk menjebak Anda. Hacker menggunakan celah keamanan yang didokumentasikan di ActiveX untuk masuk ke komputer Anda dan mencuri informasi berharga yang ditemukan di sana.

## Secara Offline

Cara kerja hacker yang berikutnya adalah cara kerja hacker secara online (dari catatan seorang sahabat yang begitu tegar [Ulygiznawati](#))

Mendengar kata password pasti kita semua setuju kalau kata tersebut berhubungan dengan sesuatu yang rahasia, penting dan tentunya tidak boleh diketahui oleh siapapun. Mengamankan data penting dengan password merupakan cara yang efektif untuk menghindari tangan-tangan jahat yang tidak berkepentingan. Banyak orang berpikir bahwa data yang telah diberi password itu aman. Tentu saja itu tidak 100% benar. Cukup mudah bagi seorang hacker untuk menjebol password karena hacker selalu memiliki cara untuk melakukannya. Namun, kita tidak bisa langsung mengganggu hacker itu jahat, banyak juga yang baik.

Terlepas dari itu semua, justru kecerobohan biasanya terjadi dari si pengguna password tersebut. Banyak yang membuat password dengan profil pribadinya. Misalnya, nama istri, nama pacar, tanggal kelahiran, nama binatang kesayangan, atau suatu kegemaran tertentu. Alih-alih supaya mudah diingat, hal itu justru menjadi bumerang bagi dirinya sendiri.

Ada beberapa **cara kerja hacker** atau metode yang biasa digunakan para hacker untuk menjebol password, yaitu:

### 1. Cara Teknis.

Dengan cara teknis, berarti kita menggunakan software untuk membongkar atau menjebol password. Misalnya saja untuk membaca file yang berformat MS Word dan tidak bisa dibuka karena harus dimasukkan password. Kita bisa menggunakan software seperti Word Password Recovery yang bisa kita download di internet. Kita bisa menggunakan Google untuk mencarinya.

Metode teknis yang biasa digunakan antara lain, adalah:

#### \* **Brute Force.**

adalah metode pencarian password dengan mencoba segala kemungkinan yang ada. Ada juga cara lain yang biasanya juga dilakukan oleh [software](#), yaitu metode Dictionary. Setiap kata dalam dictionary (kamus) yang tersimpan akan dicocokkan dengan password-nya. Jika cocok dengan password-nya, maka itulah password-nya.

Metode Brute Force mencoba segala karakter yang ada. Misalnya, dengan mencoba segala kemungkinan dari AAAAA sampai ZZZZZ atau 1,2,3,4,5,6,7,8,9. Bisa juga dengan simbol @!#\$%&\*()\_":?><+=}{. Dengan begitu, akan ditemukan password yang diinginkan.

#### \* **Keylogging.**

adalah sebuah metode untuk mengumpulkan, mencatat, dan mengoleksi apa saja yang ditekan di keyboard oleh user (target/korban). Perangkat untuk melakukan Keylogging ini dinamakan Keylogger. Keylogger ada yang berupa software dan ada juga yang berupa hardware. Keylogger yang berupa software berarti kita memasang software Keylogger pada komputer korban, kemudian software tersebut akan mencatat tombol apa saja yang ditekannya. Tools yang biasa digunakan adalah 007 Keylogger.

Keylogger hardware biasanya berupa perangkat keras (konektor) antara keyboard dan komputer. Keyboard akan dihubungkan dulu ke Keylogger baru ke komputer. Dengan begitu, kita akan mengetahui tombol apa saja yang ditekan oleh si korban dan tentu saja kita bisa mengetahui password apa yang diketikkan. Akan tetapi, jika si korban melakukan copy paste untuk password-nya, ini tentunya sudah lain cerita.

**\* Network Sniffing.**

adalah metode untuk mengetahui password dengan memantau lalu lintas paket yang keluar masuk pada sebuah LAN. Dengan demikian, apabila ada user yang memasukkan password pada sebuah situs, akan tercatat oleh tools pemantau tersebut. Misalnya, password di Facebook atau Yahoo! Mail. Tools yang bisa kita gunakan contohnya Wireshark, Ace Password Sniffer, Cain & Abel, dan Brutus. Cara Non-Teknis.

**2. Cara non-teknis** berarti tidak berhubungan langsung dengan perangkat komputer atau tools tertentu. Cara non-teknis sebenarnya lebih ke arah pendekatan (social engineering). Misalnya saja dengan mengobrol, namun secara tidak langsung. Misalnya, tanyakan korban tentang sistem operasi yang digunakan, nama istrinya, nama anaknya, nama pacarnya, tanggal lahirnya, binatang kesayangan, makanan kesukaan, atau apapun yang berkaitan dengan si korban yang sifatnya statis alias tidak berubah-ubah. Setelah mendapatkan semuanya itu, kita bisa mencoba menebak password sebagaimana keterangan yang telah kita dapatkan dari si korban. Demikianlah artikel tentang [cara kerja hacker](#), semoga bermanfaat.