

□

Petikan dari Majalah PC (Mac 2008)

Adakalanya kita melihat orang menampal maklumat sulit - seperti login dan kata laluan mereka (*password*)

- di bahagian bawah monitor PC, menggunakan nota berpelekat. Kecuaian seperti ini sebenarnya mendedahkan maklumat sulit itu kepada sesiapa sahaja yang melihatnya. Bahkan sesiapa sahaja boleh menyamar (dengan menggunakan kata laluan itu) untuk mengakses PC, rangkaian, atau sumber lain yang dibenarkan. Nyata sekali, ini telah melanggar aspek keselamatan dan mencuri identiti orang lain boleh dianggap satu jenayah.

Perkara seperti ini boleh berlaku kerana kecuaiannya, sambil lewa atau merasakan kata laluan itu tidak penting. Apa yang pasti, kata laluan adalah kunci untuk sesuatu akaun. Jika ia dibiarkan terdedah, sudah pasti akaun itu tidak selamat dan boleh diakses oleh sesiapa sahaja. Ini termasuklah rakan sekerja, pelawat, atau sesiapa sahaja yang berniat tidak baik untuk menyalahgunakannya. Tidak kira bagaimana anda menganggapnya, ia adalah pelanggaran aspek keselamatan yang serius malah berpotensi menyebabkan kejadian tidak diingini.

Selain melindungi kata laluan tersebut, anda perlu menjadikannya lebih kukuh dan menukarkannya selalu, jika dirasakan perlu. Seboleh-bolehnya, kata laluan anda tidak mengandungi maklumat peribadi seperti nama dan tarikh lahir. Kata laluan juga tidak sepatutnya berisi maklumat yang mudah diteka, berulang atau secara berturutan (seperti "111111", "123456", "abc123"). Elakkan menggunakan kata laluan yang terdiri daripada tiga huruf sahaja kerana kata laluan dianggap lemah jika terdiri daripada kurang enam aksara (panjangnya).

MEMBINA KATA LALUAN YANG KUKUH

Mencipta & Menjaga Katalaluan

Ditulis oleh Pentadbir Emel

Rabu, 23 Disember 2009 21:40 - Terakhir dikemaskini Rabu, 24 Mac 2010 08:34

Anda sedia maklum apa yang tidak wajar dilakukan. Sekarang, anda perlu tahu teknik mencipta kata laluan yang kukuh. Bagi memastikan perlindungan maksimum, kata laluan anda patut memiliki panjang sekurang-kurangnya lapan aksara. Microsoft mencadangkan sekurang-kurangnya enam aksara, tetapi jika lapan aksara sudah pastinya lebih sukar untuk dipecahkan. Bagi keselamatan yang optima, kata laluan juga patut mengandungi campuran aksara “alpha numerical” yang meliputi huruf kecil dan besar selain aksara khas seperti !#%\$&.

Lebih baik lagi jika anda tidak menggunakan perkataan sebenar tetapi hanya menggunakan aksara tertentu secara rawak. Lebih rawak susunan aksara yang digunakan, maka lebih selamat dan kukuh kata laluan yang dicipta itu. Satu contoh kata laluan yang selamat adalah seperti “Hgs3@4j55nKXls!”. Kata laluan ini adalah sepanjang 15 aksara dan mengandungi kombinasi angka, simbol, huruf (besar dan kecil). Selain itu, penggunaan kata laluan yang lebih panjang dan rawak, akan menyukarkan usaha untuk “memecahkannya”.

Apa yang mengecewakan, ramai pengguna tidak mematuhi peraturan ini. Alasannya mudah – kata laluan yang mematuhi aspek keselamatan biasanya dianggap rumit untuk kebanyakan orang mengingatnya, tanpa perlu mencatatkannya. Ini memang ada betulnya, tetapi kata laluan yang kukuh juga tidak sepatutnya sukar untuk diingati – cuma pastikan ia sukar untuk diteka. Jadi, untuk menolong anda membina kata laluan yang dianggap kukuh tetapi mudah diingatnya, berikut adalah beberapa teknik yang boleh diamalkan.

- Bentuk huruf – sesetengah nombor itu memiliki bentuk yang menyerupai bentuk huruf dan begitulah sebaliknya. Contohnya, nombor “1” kelihatan seperti huruf “l” atau “I”. Jadi, dengan menggantikan nombor yang menyerupai huruf dapat memastikan kata laluan anda tidak dicari menerusi kamus dalam talian. Contohnya, nombor “5” mirip “S”, “2” boleh menyerupai “Z” dan “3” berbentuk “E” terbalik.
- Gantikan huruf/nombor dengan aksara khas – anda juga boleh menggantikan huruf besar “S” dengan tanda “\$” dan huruf “l” atau “I” dengan tanda “!”. Anda juga boleh menggunakan versi simbolik untuk sesuatu perkataan. Contohnya perkataan “dollar” digantikan dengan simbol “\$”. Perkataan “and” digantikan dengan simbol “&”, perkataan “at” digantikan dengan simbol “@”.
- Adunan perkataan – anda mampu mencipta kata laluan berdasarkan perkataan atau frasa mudah yang dirasakan relevan. Kemudian anda boleh “mengadun” perkataan/frasa tersebut menggunakan nombor atau aksara khas. Contohnya, anda menonton sebuah filem berjudul “The War at Home”. Dengan berdasarkan kepada frasa tersebut, anda boleh mencipta kata laluan yang bagus seperti “War@H0m3”.
- Movie atau petikan kegemaran – anda boleh membina kata laluan berdasarkan kepada sesebuah lagu, wayang atau petikan kata-kata yang anda gemari. Katakan anda membuang huruf pertama untuk setiap perkataan itu, hingga 8 perkataan semuanya dan huruf yang selebihnya perlu diketepikan. Contohnya, movie berjudul seperti “Star Wars: The Empire Strikes Back, Episod 5” boleh dijadikan “SWt3\$be5”.
- Adunan bahasa – bagi mereka yang bernasib baik mengetahui dan memahami dua bahasa, anda boleh mengadun dua perkataan daripada bahasa berbeza, selain bahasa asing, anda

Mencipta & Menjaga Katalaluan

Ditulis oleh Pentadbir Emel

Rabu, 23 Disember 2009 21:40 - Terakhir dikemaskini Rabu, 24 Mac 2010 08:34

juga boleh menggunakan bahasa daerah, bahasa dialek (selalunya tiada dalam kamus) asalkan perkataan/bahasa berkenaan boleh ditaip menggunakan huruf roman. Jadi, anda bolehlah membentuknya menjadi kata laluan yang kreatif.

Sebagai langkah berjaga-jaga, anda boleh menukar kata laluan tersebut dalam tempoh tertentu seperti 90 hari. Pertukaran yang lebih kerap mungkin lebih baik, tetapi jika terlalu kerap mungkin menimbulkan kekeliruan apabila cuba mengingatnya. Komputer pelayan (*server*) di dalam rangkaian boleh dikonfigurasi untuk mengingatkan anda apabila kata laluan hampir luput dan akan meminta anda menukarnya apabila tiba masanya. Dalam banyak kes, anda diberikan tempoh selama 14 hari bagi menukar kata laluan tersebut.

Penciptaan kata laluan yang kukuh boleh menolong melindungi PC, data peribadi dan rangkaian komputer anda daripada dicerobohi pihak yang tidak diizinkan. Namun, perlindungan kata laluan tersebut tidak akan bermakna jika ia ditulis dan didedahkan di mana-mana lokasi hingga orang lain mengetahuinya. Perlu juga diingatkan bahawa penciptaan dan pengurusan kata laluan yang betul bukanlah terlalu sukar. Apabila ingin mencipta kata laluan, jangan lupa peraturan ini – mudah diingat, sukar diteka, dan jangan sesekali dikongsi.

MENGGUNAKAN APLIKASI KATA LALUAN

Tidak dinafikan sesetengah pengguna menghadapi masalah untuk mengendalikan kata laluan. Tambah pula jika mereka terpaksa menggunakan pelbagai kata laluan untuk pelbagai akaun atau khidmat yang berlainan. Ini tidak mustahil kerana ramai pengguna perlu mengakses PC di rumah dan di pejabat. Selain itu, mereka juga perlu mengakses internet, menggunakan aplikasi e-mel dan aplikasi rangkaian atau aplikasi web yang lain. Jika ia melibatkan banyak aplikasi, ada kemungkinan mereka menggunakan kata laluan yang berbeza.

Hari ini ramai yang menggunakan aplikasi berasaskan web seperti e-mel, blog, storan fail, dan sebagainya. Sesetengah khidmat akan menghantar login dan kata laluan kepada e-mel penggunanya selepas mendaftar, untuk disimpan. Selain khidmat berasaskan web tadi, ada juga yang menggunakan enkripsi untuk mengunci fail atau folder tertentu yang disimpan dalam PC dan storan mudah alih dengan kata laluan. Malah ada juga yang menggunakan kata laluan untuk mencipta fail selamat seperti fail PDF atau yang dimampatkan (zip).

Sehubungan itu, mereka bermasalah untuk mengingati banyak kata laluan. Jika begitu, anda mungkin boleh menggunakan pelbagai aplikasi penyimpanan atau pengurus kata laluan. Anda tidak perlu membelinya kerana terdapat pelbagai perisian seumpamanya yang boleh diperolehi dan digunakan secara percuma. Contohnya, aplikasi Steganos Locknote dilindungi dengan kata

Mencipta & Menjaga Katalaluan

Ditulis oleh Pentadbir Emel

Rabu, 23 Disember 2009 21:40 - Terakhir dikemaskini Rabu, 24 Mac 2010 08:34

lalu untuk menyimpan maklumat sulit termasuk kata laluan untuk aplikasi lain. Selain itu ia tidak perlu dipasang dan mudah dipindahkan ke mana-mana lokasi.

Jadi, anda boleh menyimpan pelbagai kata laluan ke dalam aplikasi tersebut. Sebaik-baiknya, nyatakan juga maklumat lain yang berkaitan seperti login, nama panggilan (username) dan nama aplikasinya. Langkah ini bertujuan untuk menyenangkan anda merujuknya kelak. Seboleh-bolehnya elakkan penggunaan kata laluan yang terlalu banyak kerana ia boleh mengelirukan. Selepas menyimpan kata laluan dan maklumat sulit lain ke dalam aplikasi berkenaan, gunakan kata laluan yang kukuh dan selamat untuk melindungi segala isinya. Jika anda terlupa kata laluan utamanya, sudah pasti segala yang tersimpan dalam aplikasi itu gagal diakses.

Tips: [Pengurusan Katalaluan](#)