BULETIN ICT
UNIT TEKNOLOGI MAKLUMAT, HOSPITAL LABUAN

780863 185779

Bil. 1/2014
Percuma

Tatacara Penggunaan emel 1GovUC

Ramai yang sedia maklum bahawa emel MOHCube sudah tidak digunakan lagi dan telah diganti dengan emel 1GovUC baru-baru ini. Disebabkan emel ini agak baru bagi pengguna emel, masih ada yang tidak faham bagaimana hendak menggunakannya.

Apa yang perlu ada buat ialah dengan membuka pelayar internet. Anda boleh menggunakan sama ada :

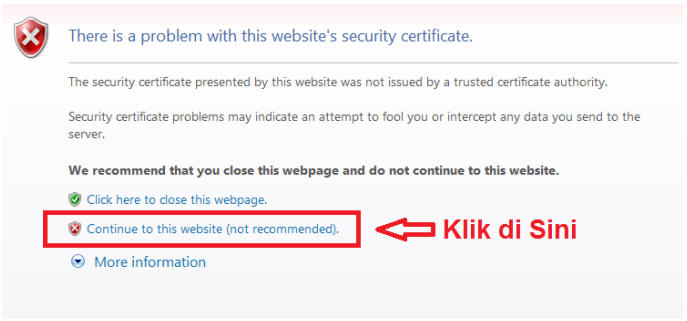
Taipkan seperti berikut di ruangan alamat :

Selain daripada itu, anda juga boleh menggunakan pautan yang terdapat di portal Hospital Labuan seperti gambar di bawah:

Untuk masuk ke portal Hospital Labuan, anda perlu menaip alamat berikut :

Ada sesetengah pelayar internet akan keluar 'certificate error' seperti berikut :

Certificate Error bagi

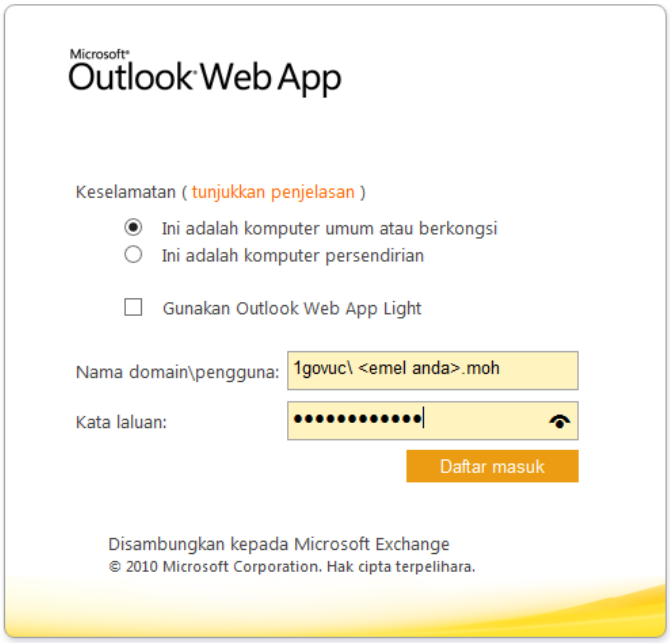


Certificate Error bagi

Certificate Error bagi

Sekiranya berlaku demikian, sila klik di tempat yang ditanda dengan petak berwarna merah.

Setelah itu, paparan seperti berikut akan terpapar.



Sila masukkan nama domain/pengguna dan katalaluan yang betul.

Contoh:
Emel anda : selamat@moh.gov.my

Nama domain\pengguna :
1govuc/selamat.moh.

Seterusnya masukkan katalaluan anda dan klik pada Daftar masuk

Emel anda sudah boleh diakses.

Awas! Peringatan Kepada Pengguna Android

Kadang-kala peralatan canggih boleh diubah menjadi perumah kepada penjenayah keselamatan maya. Tetapi bagaimana pengguna dapat mengelakkan 'jangkitan' dan 'perebakan' yang berlaku dalam telefon pintar atau komputer tablet?

Biasanya apabila anda berfikir mengenai virus, spyware atau apa-apa ancaman keselamatan siber, tentu saja anda terfikirkan mengenai komputer peribadi. Kerana majoriti serangan siber biasanya berlaku dalam komputer peribadi. Malware di telefon mudah alih? Atau komputer tablet? Bolehkah berlaku? Sememangnya boleh berlaku terutamanya jika peralatan mudah alih anda menggunakan sistem operasi seperti Android.

Menurut Juniper Networks, contoh malware Android meningkat dengan mendadak sehingga 472 peratus dalam tempoh Julai sehingga November 2011. Penggodam telah mengisytiharkan perang terhadap Android dan sebagai pengguna mungkin mereka terkena tempiasnya.

Bak kata Sun Tzu dalam Seni Peperangan, 'jika anda kenal musuh anda, anda boleh menang beratus-ratus peperangan tanpa kalah'.

Di sini terdapat lima musuh utama yang perlu pengguna Android ketahui dan bagaimana untuk mengalahkan mereka dalam permainan ini.

SMS Trojans

Menurut laporan Juniper yang sama, hampir separuh aplikasi seakan-akan Android yang berniat jahat yang beredar sekarang adalah SMS Trojan yang menghantar mesej teks dalam latar belakang (tanpa pengetahuan pengguna) kepada beberapa nombor telefon yang dimiliki penggodam.

Akibatnya sebagai pengguna anda terbeban dengan bil bulanan yang melambung. Jalan terbaik untuk menghentikan SMS Trojan adalah dengan mengelak terkena jangkitannya.

Justeru gunakan bantuan keselamatan Android yang direka khusus bagi memerangi semua serangan yang menimbulkan anca-

man. Jangan menggunakan aplikasi yang kelihatan mencurigakan atau kelihatan amat sempurna dan baik.

Carrier IQ

Penghujung tahun 2011, penyelidik mendapati rootkit pembangun perisian Carrier IQ beroperasi pada berjuta-juta peralatan mudah alih. Walaupun kelihatan tidak mencurigakan, kod berkenaan dilaporkan merekodkan lokasi termasuk kata laluan.

Malangnya semua ini berlaku tanpa pengetahuan pengguna dan tanpa pilihan melumpuhkan penggunaanya. Bagi mengawal ancaman berkenaan dapatkan Carrier IQ Test, aplikasi percuma yang dapat mengesan dan membuang perisian yang tidak dibenarkan.

Aplikasi Preloaded

Biasanya telefon pintar atau tablet didatangkan dengan bonus seperti aplikasi, perisian yang tidak termasuk dengan Android tetapi telah ditambah oleh pengilang.

Disember tahun lalu, penyelidik mendapati terdapat aplikasi preloaded yang mendedahkan keselamatan pengguna seperti yang biasa digunakan untuk mencuri data peribadi atau mencuri dengar perbualan telefon. Atau lebih teruk lagi kerana kebanyakan aplikasi 'diadun' bersama-sama OS dan tidak boleh dibuang.

Jika pengguna menggunakan Android 4.0 (Ice Cream Sandwich), mereka boleh menyembunyikan dan melumpuhkan aplikasi bloatware. Hanya dengan masuk ke Settings, Device, Apps, pergi ke All kemudian aplikasi yang mahu dibuang dan tekan Disable.

Kedai palsu Google Play

Awal tahun, Google telah mengubah Android Market kepada Google Play di mana ia menggabungkan beberapa perkhidmatan seperti aplikasi, muzik, e-book.

Bagaimanapun penjenayah siber mula mencipta domain Google Play palsu bagi menipu pengguna memasang aplikasi berbahaya. Cara melawan ancaman berkenaan adalah dengan menjadi lebih pintar.

Jangan memasang aplikasi Google Play dengan memuat turun sendiri tapi ikutlah peraturan biasa untuk mengemaskini peralatan OS. Perisian keselamatan Android boleh mengesan dan membuang segala aplikasi mencurigakan yang mungkin dipasang tanpa pengetahuan.

Jadi lebih baik gunakan anti-malware pada peralatan mudah alih.

Peringatan palsu

Jika anda mendapat mesej daripada bank berbunyi 'Akaun anda bermasalah! Kemaskini kata laluan.' Pergi ke link berkenaan membawa pengguna ke laman web yang sama dengan bank yang anda selalu lawati. Jika pengguna masuk ke akaun berkenaan, ia akan membuka laluan menjadi mangsa jenayah siber mencuri semua data peribadi pengguna.

Jangan sekali-kali masuk ke link yang terdapat di dalam e-mel atau mesej teks walaupun kelihatan memang sama. Pastikan anda buka perayauan dan sambung kepada institusi kewangan secara terus dan pastikan URL bermula dengan https:// dan kini beberapa institusi kewangan yang mempunyai pelbagai langkah-langkah keselamatan bagi menjaga hak pengguna. Dan jika pengguna masih ragu-ragu mengenai keselamatan, hubungi institusi kewangan untuk berurusan secara terus.

Sumber : www.nizarazu.com

Apa Itu Virus Trojan Horse?

Virus Trojan Horse ialah program yang menjangkiti sesuatu komputer untuk mengakibatkan kerosakan. Kerosakan tersebut boleh ditafsirkan sebagai kecurian data, kecurian identiti, akaun sulit dan sebagainya. Trojan Horse boleh menjangkiti mesin pengguna tanpa disedari. Sebaik sahaja ia menembusi komputer, *virus Trojan Horse* akan mengimbas keseluruhan komputer dengan matlamat untuk mencuri data peribadi.

Salah satu virus Trojan Horse terawal dikesan pada tahun 1980-an, apabila beberapa komputer terjejas akibat jangkitannya. Ia telah dibangunkan oleh penggodam dengan tujuan untuk mencuri kata laluan akaun-akaun peribadi atau sulit. Semakin hari ia semakin berkembang dan semakin canggih fungsinya.

Nama Trojan Horse datang dari cerita mitologi Yunani tentang pengepungan Troy. Orang-orang Yunani tidak mampu untuk menakluk bandar sehingga mereka membina sebuah kuda kayu Trojan yang besar dan menyembunyikan beberapa orang pahlawan (tentera) di dalamnya. Kuda kayu itu sepatutnya menjadi hadiah dari orang Yunani, memaklumkan bahawa mereka akan belayar dan tidak lagi mahu menakluki bandar. Apabila kuda Trojan dibawa masuk ke dalam bandar, tentera Yunani di dalamnya menunggu sehingga hari beransur gelap dan kemudian menyerang Troy, memusnahkan sekali gus menangi peperangan.

Menurut beberapa sumber dalam talian, virus Trojan Horse pertama dikenali sebagai ‘pest trap’, yang juga dikenali sebagai ‘Spy Sheriff’.Virus Trojan Horse ini berjaya menjangkiti kira-kira sejuta komputer di seluruh dunia. Ia tidak merosakkan mana-mana fail pada komputer, sebaliknya ia membawa kepada kemunculan sejumlah besar pop-up, sebahagian besar daripadanya kelihatan seperti amaran kepada pengguna mengenai keperluan untuk memasang beberapa jenis aplikasi/perisian. Apabila virus Trojan Horse menjangkiti satu-satu komputer, agak sukar untuk membuangnya. Jika ia mahu dipadam, virus Trojan Horse hanya akan memasang semula dirinya daripada data fail tersembunyi yang telah terjejas (dijangkiti) pada komputer.

Terdapat satu perkara penting yang perlu diingat, virus Trojan Horse tidak boleh ‘dihidupkan’ melainkan jika pengguna tidak mengaktifkan program yang mempunyai virus tersebut. Adalah penting yang anda tidak memuat turun program-program yang tidak diketahui, yang mana sumber integritinya boleh diragui, lebih-lebih lagi jika seseorang atau sesuatu memujuk anda untuk berbuat demikian.

Sumber : www.nizarazu.com