

OUCH!

DALAM ISU KALI INI...

- Lindungi Diri Anda
- Lindungi Komputer/Akaun Anda
- Untuk Ibu Bapa

'Gaming' Dalam Talian Secara Selamat

Gambaran Keseluruhan

'Gaming' atau permainan dalam talian merupakan cara yang baik untuk berhibur, walau bagaimanapun ia mempunyai risiko tersendiri yang unik. Dalam artikel ini, kami akan memberitahu anda apa yang boleh dilaksanakan untuk melindungi keluarga dan diri anda semasa bermain dalam talian.

Melindungi Diri Anda

Apa yang membuat permainan dalam talian begitu menarik ialah anda boleh bermain dan berkomunikasi dengan orang lain di seluruh dunia. Selalunya anda tidak mengenali orang yang sedang bermain dengan anda. Walaupun sebahagian besar orang dalam talian ingin berhibur sama seperti anda, terdapat segelintir yang mahu membuat keburukan. Berikut adalah beberapa perkara yang perlu anda amalkan untuk keselamatan.

- Berhati-hatilah dengan mesej yang meminta anda untuk mengambil tindakan seperti mengklik pada pautan atau memuat turun fail. Sama seperti serangan "phishing", penjenayah akan cuba untuk menipu atau memperdaya anda supaya mengambil tindakan yang boleh menjangkiti komputer anda. Jika terdapat sebarang mesej yang kelihatan ganjil, segera, atau terlalu indah untuk dipercayai, berwaspadalah kerana ia mungkin serangan siber.
- Banyak permainan dalam talian mempunyai pasaran kewangan mereka sendiri di mana anda boleh berniaga, bertukar atau pun membeli barang-barang maya. Sama seperti di dunia sebenar, terdapat penipu dalam sistem ini yang akan cuba untuk memperdaya untuk mendapatkan wang anda atau cuba untuk mencuri secara terang-terangan.
- Berhati-hati apabila bertransaksi menggunakan wang untuk membeli barangan secara maya dan begitu juga sebaliknya. Anda dinasihatkan untuk bertransaksi menggunakan wang hanya di pasaran yang mempunyai reputasi baik.
- Hadkan maklumat anak-anak anda serta anda sendiri di laman talian. Jangan sekali-kali berkongsi maklumat peribadi seperti kata laluan atau alamat rumah.
- Banyak laman sesawang, seperti perbankan dalam talian yang menggunakan soalan keselamatan untuk pengesahkan identiti. Penyerang mendapat jawapan kepada soalan keselamatan tersebut dengan berkawan dengan mangsa di permainan dalam talian. Anda harus ingat bahawa anda tidak perlu menjawab sebarang pertanyaan orang semasa bermain dalam talian.

Editor Jemputan

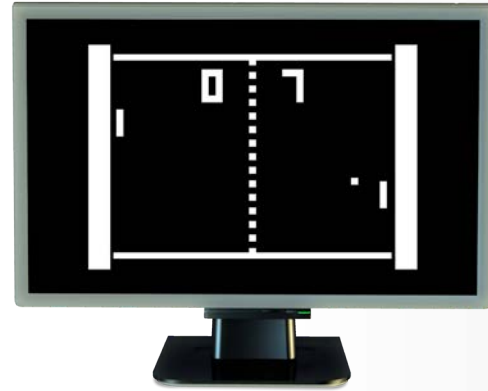
Jake Williams adalah pengasas dan perunding utama di Rendition Infosec, pengajar yang diperakui oleh SANS dan penulis bersama beberapa kursus SANS. Beliau aktif di laman Twitter sebagai [@MalwareJake](https://twitter.com/MalwareJake) dan kerap menulis di malwarejake.blogspot.com.

'Gaming' Dalam Talian Secara Selamat

Lindungi Sistem/Akaun Anda

Langkah seterusnya adalah untuk melindungi komputer yang anda gunakan. Penjenayah akan cuba untuk mengambil alih komputer atau akaun permainan anda dan anda perlu melindunginya.

- Gunakan kata laluan yang kukuh untuk komputer dan semua akaun permainan anda. Dengan cara ini, penyerang tidak boleh meneka kata laluan untuk mengambil alih akaun anda. Jika permainan anda menawarkan "two-step verification", gunakannya. Selain itu, pastikan setiap akaun permainan anda mempunyai kata laluan yang berbeza. Sehubungan itu, jika satu akaun dikompromi, akaun anda yang lain masih selamat.
- Lindungi komputer anda dengan sentiasa menggunakan versi terbaru sistem operasi dan juga perisian permainan. Sama seperti sistem operasi dan aplikasi laman sesawang, perisian permainan lama dan ketinggalan zaman selalunya telah diketahui kelemahannya oleh penyerang yang boleh mengeksploitasi dengan menggodam komputer anda. Dengan mengemaskini aplikasi komputer dan permainan anda, anda menghapuskan sebahagian besar kelemahan yang mereka ketahui.
- Gunakan "anti-virus", pastikan ia dikemaskini dan periksa mana-mana program fail yang anda jalankan dalam masa nyata.
- Muat turun perisian permainan dari laman sesawang yang dipercayai. Jika anda memuat turun perisian permainan, pastikan anda memuat turun dari laman sesawang penjual atau beberapa lokasi terkenal lain yang dipercayai. Selalunya penyerang siber akan mencipta perisian permainan versi palsu atau berjangkit, kemudian mengedarkannya dari "server" mereka sendiri. Jika anda memasang salah satu perisian permainan ini, penjenayah akan mempunyai kawalan penuh terhadap komputer anda.
- Permainan pek tambahan, sering dibangunkan oleh komuniti pemain yang selalu digunakan untuk menambah ciri-ciri baharu. Penyerang mungkin akan menjangkiti pek tambahan permainan ini dengan "malware" yang sangat sukar untuk dikesan oleh "anti-virus". Sama seperti anda memuat turun permainan, pastikan anda memuat turun pek tambahan ini dari lokasi yang dipercayai juga. Di samping itu, jangan gunakan pek tambahan jika ia memerlukan anti-virus dimatikan atau membuat sebarang perubahan kepada peranti keselamatan anda.
- Pasaran gelap telah muncul untuk menyokong aktiviti penipuan. Selain tidak beretika, program ini merupakan "rootkit", sejenis "malware" yang paling bahaya. Jangan sekali-kali memasang atau menggunakan mana-mana jenis perisian palsu.
- Periksa laman sesawang atau apa-apa jua perisian permainan dalam talian yang anda gunakan. Banyak laman permainan mempunyai bahagian untuk melindungi sistem dan diri anda, pastikan anda mengamalkan saranan mereka.
- Akhir sekali, sentiasa berhati-hati semasa bermain dalam peranti mudah alih seperti bermain di komputer anda. Penyerang siber mula menyasarkan peranti mudah alih.



Kunci untuk kekal selamat semasa bermain permainan dalam talian ialah menggunakan kata laluan yang kukuh, melindungi komputer dan menggunakan akal fikiran ketika berkomunikasi dengan orang yang tidak dikenali atau apabila anda menerima mesej dalam talian yang ganjil atau berbentuk permintaan.

'Gaming' Dalam Talian Secara Selamat

Untuk Ibu Bapa

Jika anda adalah ibu bapa, pastikan anak-anak anda mengikuti langkah-langkah yang digariskan di atas (untuk kanak-kanak yang lebih muda, anda mungkin perlu melaksanakan langkah-langkah tersebut untuk mereka). Di samping itu, terangkan mengenai risiko permainan dalam talian kepada anak-anak anda. Pendidikan dan dialog terbuka dengan anak-anak anda merupakan salah satu langkah paling berkesan yang boleh diambil untuk melindungi mereka. Salah satu cara pilihan kami supaya anak-anak berkomunikasi adalah dengan meminta mereka menunjukkan bagaimana permainan mereka berfungsi, minta mereka mengajar anda mengenai permainan dalam talian tersebut dan menunjukkan kepada anda bagaimana permainan biasa kelihatan. Malahan, anda boleh juga bermain dengan mereka. Di samping itu, minta mereka menggambarkan orang yang mereka bertemu dalam talian. Selalunya permainan dalam talian menjadi sebahagian besar daripada kehidupan sosial anak anda. Dengan bercakap kepada mereka (dan meminta mereka bercakap dengan anda) anda boleh mengesan jika terdapat sebarang masalah dan melindungi mereka dengan lebih berkesan daripada sebarang teknologi.

Mari Belajar Lebih Lanjut!

Langganilah surat berita bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer OUCH!, akseslah arkib OUCH!, dan belajar lebih lanjut mengenai penyelesaian kesedaran keselamatan SANS dengan melayari laman sesawang kami di <http://www.securingthehuman.org>.

Penterjemahan oleh SNSC.

Pusat Keselamatan Rangkaian SKMM (SKMM Network Security Centre- SNSC) beroperasi di bawah Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) dengan matlamat menjamin keselamatan maklumat, kebolehpercayaan dan keutuhan rangkaian di Malaysia. Laman Web: <http://snc.skmm.gov.my/>.

Sumber

Kejuteraan Sosial:	http://www.securingthehuman.org/ouch/2014#november2014
Serangan "Phishing":	http://www.securingthehuman.org/ouch/2013#february2013
Kata Laluan:	http://www.securingthehuman.org/ouch/2013#october2013
Apakah itu "Anti-Virus"?:	http://www.securingthehuman.org/ouch/2014#december2014
StaySafe Online:	http://www.staysafeonline.org/stay-safe-online/for-parents/gaming-tips

OUCH! diterbitkan oleh program SANS "Securing The Human" dan diedarkan di bawah lesen [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Kebenaran diberikan untuk mengedarkan surat berita ini atau menggunakannya dalam mana mana program kesedaran selagi tiada perubahan dibuat kepada kandungan asal.

Editor: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Translated by: Muhamad Hashimi, Rahayu Aziz, and Sheikh Ahmad Raffie



securingthehuman.org/blog



[/secrethehuman](https://www.facebook.com/secrethehuman)



[@secrethehuman](https://twitter.com/secrethehuman)



[securingthehuman.org/gplus](https://plus.google.com/securingthehuman)