Waspada dan Peduli terkait keamanan informasi dalam memanfaatkan internet

Directorate of
INFORMATION SECURITY
Directorate General of Informatics Applications

https://www.kominfo.go.id/

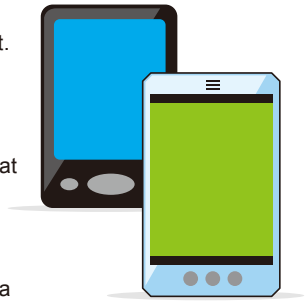
ASEAN · JAPAN
Information Security Awareness

Peduli, Aman dan Waspada

Keamanan Informasi

Manfaatkan internet dengan bijaksana

Keamanan Telepon Pintar



Smartphone saat ini sangat populer di seluruh dunia, dan persentase smartphone dalam penjualan ponsel juga meningkat.

Smartphone merupakan perangkat yang sangat canggih dibandingkan dengan telepon selular tradisional yang memungkinkan kita untuk melihat situs yang dirancang untuk Komputer Pribadi (PC) serta berbagai macam aplikasi yang dapat didownload dan digunakan secara bebas.

Versi terbaru dari Sistem Operasi*1 dan aplikasi*2 pada smartphone umumnya tersedia secara berkala. Pembaruan/update*3 aplikasi mungkin memberikan lebih banyak fungsi serta meningkatkan kecanggihan atau keamanan aplikasi smartphone.

*1 - OS adalah singkatan dari sistem operasi yang merupakan perangkat lunak yang mengontrol PC atau smartphone. Misalnya pada PC, OS mengelola berbagai macam fungsi seperti I / O (Input / Output) yang berfungsi mengelola input dari keyboard, atau output untuk menampilkan, atau fungsi printer.

*2 - Aplikasi adalah perangkat lunak untuk tujuan tertentu, seperti pengolah kata, atau membuat spreadsheet. Pengguna dapat memilih aplikasi yang mereka butuhkan, dan menggunakan mereka setelah mereka bangun di OS yang memiliki fungsi dasar yang umum digunakan oleh setiap perangkat lunak.

*3 - Perbarui berarti perubahan minor perangkat lunak untuk memperbaiki bug, atau menawarkan peningkatan fungsi. Dengan menerapkan fungsi tersebut, pengguna dapat menyimpan perangkat lunak selalu update. Ini juga penting untuk memperbarui perangkat lunak keamanan untuk keamanan informasi.

Resiko dan Ancaman

1 Jumlah malware pada smartphone saat ini meningkat. Jika perangkat Anda terinfeksi oleh malware, isi buku alamat atau informasi pribadi lainnya mungkin dapat terkirim ke server eksternal atau SERVER yang tidak sah.

2 Selain terinfeksi oleh malware, ketika men-download aplikasi, aplikasi dapat meminta informasi perangkat atau meminta isi buku alamat untuk dikirim ke server eksternal. Misalnya, ada kasus aplikasi yang mengaku dirancang untuk meningkatkan waktu baterai, namun sebenarnya aplikasi tersebut berfungsi untuk mencoba mengirim informasi alamat kepihak eksternal yang tidak relevan dengan penggunaan aplikasi.

Langkah Aman untuk Merespon

- Selalu perbarui Sistem Operasi, aplikasi dan perangkat lunak anti-virus pada smartphone ke versi terbaru yang tersedia. Karena smartphone berisi informasi buku alamat dan informasi sensitif lainnya, perhatian yang lebih sangat diperlukan.
- Ketika men-download aplikasi, pastikan untuk memeriksa apakah situs tersebut dapat dipercaya dan cek siapa yang menyediakan aplikasi tersebut. Kemudian saat men-download, pastikan untuk memeriksa perjanjian persetujuan dan / atau persyaratan layanan untuk informasi yang dikumpulkan dan bagaimana akan digunakan, sebelum menyetujui atau menggunakan aplikasi.

Keamanan Jaringan Nirkabel

Dalam beberapa tahun terakhir ini, Komputer Pribadi (PC) menjadi lebih ringan dari sebelumnya serta smartphone menjadi lebih populer, dimana telah mempercepat penggunaan "LAN Nirkabel" yang memungkinkan akses ke internet melalui komunikasi nirkabel di dalam dan bahkan di luar rumah atau kantor.

Selain layanan berbayar oleh para penyedia, fasiltas layanan Wi-Fi gratis yang tersedia di bandara, stasiun kereta api dan bangunan komersial meningkat.

Resiko dan Ancaman

1 Sejak LAN nirkabel di rumah atau kantor dapat dihubungkan secara bebas dalam wilayah yang dicakup oleh gelombang radio, komunikasi dapat disadap kecuali langkah-langkah PENGAMANAN yang sesuai sudah diambil.

2 Selain itu, akses tidak sah ke jaringan LAN nirkabel dapat mengakibatkan kebocoran informasi pribadi atau rahasia perusahaan, atau digunakan sebagai batu loncatan untuk menyerang server. Saat menggunakan layanan LAN nirkabel publik, PC atau smartphone dapat terhubung ke titik akses palsu. Dalam hal ini, komunikasi Anda mungkin didengar orang lain (eavesdropped) walaupun LAN nirkabel yang Anda gunakan telah dienkripsi.

Langkah Aman untuk Merespon

- Gunakan LAN nirkabel di rumah atau kantor setelah pengaturan enkripsi data seperti (WPA2: Wi-Fi Protected Access 2, dll) sehingga komunikasi teks yang jelas tidak dapat disadap dan untuk mencegah akses yang tidak sah. Ketika pengaturan secara manual enkripsi data, gunakan string karakter yang cukup panjang untuk tidak dapat dianggap sebagai kunci enkripsi.
- Ketika menggunakan layanan LAN nirkabel publik, gunakan situs yang dienkripsi dengan SSL*4 (website yang URL dimulai dari "https://") saja dan periksa PC yang Anda gunakan sebelum menggunakan layanan ini dan perikas file sharing dinonaktifkan.

*4 - SSL adalah singkatan dari Secure Socket Layer yang merupakan protokol untuk mengenkripsi data yang dikirim di web.

Penipuan dengan Satu Kali KLIK

Satu-klik penipuan mengacu pada menipu uang dengan menampilkan layar untuk tagihan untuk biaya pendaftaran atau biaya pemakaian layanan setelah mengklik gambar atau video di situs Web.

Baru-baru ini, ada penipuan “satu-klik” yang menggunakan aplikasi smartphone dan layanan media sosial seperti blog*1 / SNS*2.

Selain kasus "satu klik", layar penagihan dapat ditampilkan setelah beberapa klik seperti verifikasi usia, dll Dalam beberapa kasus lain teknik yang digunakan menjebak dan canggih, seperti layar penagihan tidak bisa hilang walaupun perangkat sudah dimatikan.

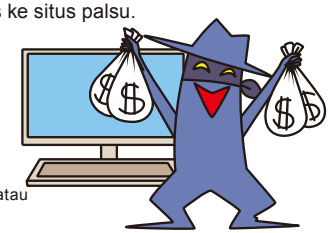
*1 - Blog adalah bentuk singkat dari Weblog dimana pengguna dapat menulis pendapat atau kesan mereka seperti jurnal, dan pengunjung dapat dengan bebas memberikan komentar mereka di posting blog tersebut

*2 - SNS adalah singkatan dari Social Networking Service yang menyediakan situs web yang memiliki banyak fungsi seperti membuka diary atau album foto kita kepada masyarakat, atau membuat masyarakat dapat bertukar pendapat secara bebas.

Resiko dan Ancaman

1 Mengklik gambar atau video yang membuat pengguna tertarik dapat menyebabkan penagihan tidak sah atau mengarahkan pengguna akses ke situs palsu.

2 Ada beberapa kasus di mana alamat IP*3 dan / atau informasi penyedia terdaftar pada layar penagihan untuk menciptakan rasa takut dengan cara membuatnya terlihat, seperti individu tersebut telah teridentifikasi.

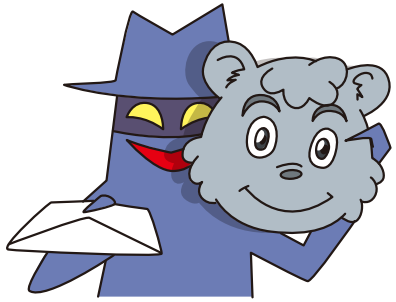


*3 - Alamat IP adalah nomor identifikasi otomatis ditetapkan ke instrumen atau komputer ketika mereka terhubung ke internet.

Langkah Aman untuk Merespon

- Usaha-usaha pemblokiran tersambungnya situs jahat (malicious sites) dengan menggunakan peranti lunak filtering atau perangkat lunak securiti terbaru lainnya. Juga pastikan untuk men-download aplikasi smartphone hanya dari situs terpercaya.
- Sadarilah bahwa ketika menggunakan komputer, satu klik saja tidak akan mengidentifikasi Anda, sehingga abaikan langkah-langkah untuk pembayaran. Untuk smartphone, berhati-hati bahwa ketergantungan pada aplikasi, informasi yang tersimpan pada perangkat seperti kontak informasi Anda sendiri atau informasi lainnya yang terdapat di buku alamat dapat terpublikasi.
- Jika Anda kebetulan untuk menghubungi salah satu situs tersebut, penagihan tidak sah terus berlanjut atau jika Anda menerima panggilan pengadilan, berkonsultasi dengan otoritas setempat (konseling administratif atau konsultasi pengacara gratis, dll) sebagai nasihat.

Target serangan surat elektronik



Serangan email yang ditargetkan adalah serangan yang email dikirim menyamar seolah-olah dikirim dari seorang kenalan pengguna, email tersebut kemungkinan akan berisi lampiran berbahaya yang ketika diakses akan menginfeksi sistem dengan virus atau trojan.

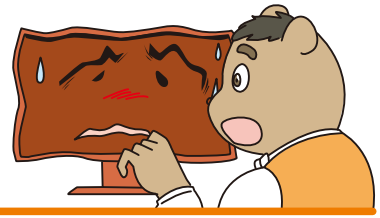
Sebuah contoh sederhana adalah target adalah organisasi tertentu atau pengguna individu. Sebuah email dengan lampiran yang terinfeksi virus dikirim dari penyerang berpura-pura pihak terkait atau rekan organisasi.

Kasus laporan password yang dicuri atau terinfeksi virus, dll disebabkan oleh serangan email yang ditargetkan.

Resiko dan Ancaman

1 Untuk modus baru serangan, metode yang digunakan semakin canggih dan maju, yaitu dengan menyamarkan sebagai email terpercaya Nama departemen dan / atau individu yang digunakan benar adanya, selain menggunakan isi atau informasi dimana hanya pihak terkait yang tahu.

2 Jika sudah tersusupi virus, kemudian bila pengguna membuka lampiran maka secara otomatis akan menyebabkan koneksi ke server eksternal yang dikehendaki penyusup dan informasi dalam komputer akan bocor.



Langkah Aman untuk Merespon

- Jangan membuka lampiran e-mail atau URL yang mencurigakan.
- Jika Anda kebetulan membuka email yang mencurigakan, jangan panik dan tidak mematikan perangkat. Lepaskan kabel jaringan dan meminta bantuan dari administrator sistem.
- Instal perangkat lunak antivirus dan pastikan selalu up to date.
- Secara berkala memperbarui aplikasi disampaing Sistem Operasi (OS).

Serangan DDoS

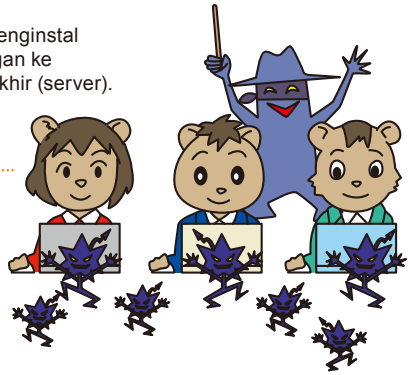
Sebuah serangan DDoS adalah serangan pada server tertentu yang dibombardir dengan paket-paket dari sejumlah besar komputer yang sudah terinfeksi (compromised) di beberapa jaringan, hingga komunikasi meluap (overload) dan server berhenti berfungsi.

DDoS: Distributed Denial of Service

Resiko dan Ancaman

1 Seorang penyerang secara diam-diam dapat menginstal program jahat tersebut untuk melakukan serangan ke komputer yang tidak terhubung dengan target akhir (server). Oleh karena itu, pengguna dapat menyerang komputer lain tanpa mengetahuinya.

2 Komputer yang terinfeksi (compromised) dapat melakukan serangan-serangan lain selain serangan DDoS seperti menginfeksi komputer lain dengan virus, mengirim email spam atau mengotori website atas nama anda sebagai penyerangnya.



Langkah Aman untuk Merespon

- Selalu perbarui ke versi terbaru Sistem Operasi (OS) pada komputer, smartphone atau perangkat lain yang akan terhubung ke internet.
- Instal perangkat lunak antivirus dan pastikan bahwa itu up to date.
- Secara berkala memperbarui aplikasi selain OS.

Etika Menggunakan Internet

Karena peningkatan penggunaan SNS (layanan jaringan sosial), masalah di internet yang sebelumnya tidak terpikir telah datang.

Ada kasus bahwa individu memposting konten di internet di mana individu yang difitnah dapat teridentifikasi atau dimana perusahaan harus mengeluarkan permintaan maaf kepada publik.

Resiko dan Ancaman

1 Ada kemungkinan di mana posting umum di SNS dapat mengakibatkan informasi pribadi terungkapkan atau pencemaran nama baik dari orang lain atau pelanggaran privasi.

2 Sebuah posting umum di internet dapat menyebabkan permintaan pembayaran atas suatu kerusakan, teguran oleh hukum atau bahkan penangkapan.

Langkah Aman untuk Merespon

- Berhati-hatilah untuk tidak mengungkapkan informasi pribadi yang tidak perlu di internet melalui SNS, blog atau miniblog, dll. Posting gambar dapat mengungkapkan informasi lokasi sehingga Anda harus berhati-hati.
- Bahkan di internet, pastikan untuk mempertimbangkan martabat dan privasi orang lain dan periksa isi sebelum posting informasi.

Pengaturan Yang Tepat Untuk ID dan Password

Untuk penggunaan email, belanja di internet, internet banking dan layanan lainnya di internet dengan aman, ada banyak jenis skema otentikasi, sedangkan yang paling populer adalah ID / password kombinasi.

Baru baru ini telah terjadi peningkatan serangan cyber dimana targetnya adalah informasi akun pengguna seperti ID dan password.

Resiko dan Ancaman

1. Pihak ketiga berbahaya (malicious third party) dapat menyamar sebagai pengguna dan dapat mengungkapkan informasi atau menyebabkan permasalahan keuangan jika kombinasi ID / password pengguna sangat sederhana (seperti tanggal lahir 4 digit, atau "9999", dll) atau jika ID / password tersebut sembarangan dikelola. (misalnya, password ditempel pada layar komputer, dll)

2. Apabila menggunakan ID / password yang sama untuk beberapa situs dan ada informasi yang bocor dari salah satu situs, maka pengguna akan menjadi korban dari akses yang tidak sah di situs lain.

Langkah Aman untuk Merespon

- Atur password dengan string sulit diduga setidaknya 8 karakter yang berisi angka, huruf dan karakter huruf kecil dan simbol. Juga gantilah password secara teratur.
- Jangan berbagi password dengan orang lain atau menggunakan password yang sama untuk beberapa situs. Jika sebuah situs yang sedang digunakan memberikan konfirmasi bahwa password telah bocor, ganti password anda tidak hanya pada situs tersebut, tetapi pada situs-situs lain yang menggunakan password yang sama.
- Hindari memasukkan informasi pribadi pada komputer umum di tempat seperti kafe internet dan tempat-tempat lainnya

Surat Elektronik Yang Berisi Spam 1

Email adalah alat komunikasi yang cukup nyaman dengan pengiriman dan penerimaan dapat dilakukan tanpa mempertimbangkan di mana penerima berada atau seberapa jauh mereka. Namun, dari sudut pandang penerima mungkin ada banyak email yang tidak perlu, pesan spam, yang dikirim dan diterima.

Karena sejumlah besar pesan adalah spam email yang dikirim, ada masalah di mana fasilitas peralatan di penyedia bisa jadi kelebihan muatan yang mana dapat menyebabkan penundaan untuk mendapatkan pesan lain yang dikirim / diterima.

Resiko dan Ancaman

1. Terdapat kasus bahwa komputer secara acak akan menghasilkan sejumlah besar alamat email dan mengirimkan pesan email tersebut. Oleh karena itu, penggunaan alamat email yang pendek dan nama-nama populer di alamat email dapat menyebabkan kemungkinan peningkatan menerima email spam.

2. Beberapa alamat email yang valid untuk mengirim email spam yang terkumpul melalui pendaftaran layanan gratis palsu atau melalui prosedur untuk berhenti berlangganan fiktif. Selain itu, membuka file lampiran di email atau mengakses link dalam email dapat menyebabkan teraksesnya sebuah website yang tidak sah atau menyebabkan infeksi virus.

Langkah Aman untuk Merespon

- Alamat email harus berisi sejumlah besar karakter dan termasuk angka acak untuk sulit ditebak.
- Jangan sembarangan masukkan alamat e-mail Anda ke situs web atau menampilkan alamat e-mail Anda di website, jika tidak perlu.
- Jika diperlukan untuk menggunakan situs yang sebenarnya tidak dapat dipercaya, mungkin sebaiknya menggunakan alamat email yang tersedia secara bebas sebagai lawan menggunakan penyedia alamat yang diberikan.

Surat Elektronik Yang Berisi Spam 2

Spam email mungkin tidak hanya menyebabkan ketidaknyamanan kepada penerima atau mengganggu bekerja, tetapi metodenya menjadi semakin berbahaya dan cerdik, yang dapat menyebabkan pengguna mengakses situs yang tidak sah di mana uangnya dapat dicuri, atau melalui pengaturan email spam filter.

Smartphone dapat terinfeksi oleh virus dalam email spam, dimanipulasi dari tempat yang jauh untuk mengirim sejumlah besar email spam tanpa pengguna mengetahuinya.

Resiko dan Ancaman

1 Terdapat kasus bahwa komputer secara acak akan menghasilkan sejumlah besar alamat email dan mengirimkan pesan email tersebut. Oleh karena itu, penggunaan alamat email yang pendek dan nama-nama populer di alamat email dapat menyebabkan kemungkinan peningkatan menerima email spam.

2 Beberapa alamat email yang valid untuk mengirim email spam yang terkumpul melalui pendaftaran layanan gratis palsu atau melalui prosedur untuk berhenti berlangganan fiktif. Selain itu, membuka file lampiran di email atau mengakses link dalam email dapat menyebabkan teraksesnya sebuah website yang tidak sah atau menyebabkan infeksi virus.

Langkah Aman untuk Merespon

- Cobalah untuk memblokir email spam dengan menggunakan penanggulangan layanan spam email seperti fungsi penolakan atau fungsi anti-spoofing oleh penyedia layanan internet atau perangkat lunak penyaringan.
- Jika Anda menerima email spam, hapus tanpa membukanya. Kemudian jangan membuka lampiran atau mengakses link dari email yang mencurigakan. Ini juga mungkin efektif untuk meneruskan email spam ke operator atau instansi publik terkait
- Ambil penanggulangan pada smartphone dan Personal Komputer (PC).

Lindungi smartphone dan komputer Anda sendiri.

Smartphone dan komputer adalah alat yang berguna, Tapi di sisi lain mereka menghadapi banyak bahaya seperti terinfeksi virus komputer. Ingatlah untuk mematuhi tiga tips keamanan informasi untuk memastikan keselamatan dan keamanan saat menggunakan komputer dan smartphone.

Tiga Petuah Penting Untuk Keamanan Informasi

Tangani informasi pribadi yang penting dengan hati-hati.

Lindungi komputer Anda dengan update keamanan terbaru.

Jangan mengakses website yang mencurigakan atau email asing.

Langkah-langkah keamanan informasi dapat disamakan dengan PEMASANGAN sabuk pengaman ketika kita pergi keluar di dalam mobil, dan itu sesuatu yang kita tidak boleh lupa ketika kita menggunakan smartphone atau komputer