

OUCH!

Buletin Bulanan Keamanan Komputer

Gawai Purnakarya

Sekilas

Gawai seperti telepon pintar, jam tangan pintar dan tablet senantiasa berkembang dan berinovasi secara cepat. Hal ini menyebabkan tidak sedikit orang berganti peralatan hampir setiap tahun sekali. Namun, orang sering tidak paham bahwa dalam sebuah gawai tersimpan banyak informasi penting. Dibawah ini akan dibahas apa saja yang mungkin tersimpan di dalam sebuah gawai dan bagaimana cara menghapusnya secara permanen sebelum dipurnakaryakan (dipensiunkan). Bila gawai Anda adalah aset perusahaan dan di dalamnya tersimpan data bisnis, pastikan menghubungi pihak terkait perihal pencadangan (backup) dan prosedur penggantian peralatan.

Informasi Anda

Banyak orang abai bahwa gawai menyimpan lebih banyak data penting, terkadang malah lebih banyak dari komputer.



- Tempat tinggal, kantor dan tempat-tempat yang dikunjungi
- Detil informasi banyak orang di direktori termasuk keluarga, famili, teman dan rekan kerja.
- Riwayat panggilan telepon keluar dan masuk, pesan suara dan telepon tak terbalas
- Sesi pengiriman pesan atau obrolan di aplikasi chat, game dan media sosial
- Riwayat penelusuran web, pencarian, cookies dan halaman cache.
- Foto-foto pribadi, video dan rekaman suara
- Sandi yang tersimpan dan akses ke berbagai akun seperti bank, media sosial atau surel
- Informasi kesehatan, termasuk umur, detak jantung, riwayat olah raga dan tekanan darah.

Hapus Bersih Gawai

Tidak peduli bagaimana cara Anda berhenti menggunakan sebuah gawai, apakah dengan cara mendonasikannya, menukarnya dengan yang lebih mutakhir, memberikannya ke famili, menjualnya atau bahkan membuangnya, Anda harus memastikan semua data penting terhapus. Tidak hanya dihapus begitu saja namun harus dipastikan semua data benar-benar musnah. Cara termudah adalah me'reset' gawai. Proses reset bisa saja berbeda di setiap gawai, cara di bawah ini adalah paduan untuk dua jenis gawai yang umum dipakai. Agar lebih aman, aktifkan fasilitas enkripsi sebelum proses reset dimulai. Di banyak gawai

terbaru, cara termudah menggunakan enkripsi adalah mengaktifkan screen lock (ayo aktifkan!). Selain itu, disarankan untuk membuat cadangan (backup) data peralatan sebelum melakukan proses reset.



- Gawai Apple iOS: Settings | General | Reset | Erase All Content and Settings
- Gawai Android: Settings | Privacy | Factory Data Reset

Kartu SIM Dan Kartu Tambahan

Tidak hanya gawai, Anda perlu memikirkan juga kartu SIM (Subscriber Identity Module). Kartu ini berguna untuk keperluan sambungan selular dan data. Saat menghapus bersih isi gawai, kartu SIM masih menyimpan beberapa informasi akun Anda. Bila nomer telepon tersebut tetap akan digunakan di gawai baru, mintalah bantuan penyedia jasa layanan telepon. Bila hal itu tidak mungkin dilakukan, hancurkan kartu SIM tersebut supaya tidak digunakan pengguna lain untuk mengakses informasi atau akun Anda. Selain itu, beberapa gawai Android menggunakan kartu SD (Secure Digital) tambahan guna menambah ruang simpan data. Lepaskan kartu ini dari gawai yang tidak akan digunakan lagi. Kartu ini biasanya masih bisa digunakan di gawai lain atau difungsikan sebagai alat penyimpan data dengan bantuan adaptor USB. Bila penggunaan ulang kartu SD tidak dimungkinkan, hancurkan kartu tersebut seperti halnya kartu SIM.

Bila Anda ragu pada langkah-langkah diatas, atau menemukan opsi reset gawai berbeda, bawa gawai Anda ke teknisi yang berpengalaman atau ke toko penjualnya. Bila Anda bermaksud membuang gawai yang sudah tidak terpakai, pertimbangkan untuk mendonasikannya. Banyak organisasi sosial berminat menerima gawai layak pakai.

Versi Bahasa Indonesia

BIPIMax memberikan Pelatihan Optimasi Proses Bisnis (LSS) dan Pengenalan Keamanan & Proteksi Informasi. Informasi lengkap: <http://www.bipimax.net>

Editor Tamu

Christopher Crowley (@CcrowMontance) adalah konsultan independen di wilayah Washington DC, dengan fokus di operasi keamanan. Beliau menulis cuitan dan blog secara berkala. Simak penerbitan bukunya dengan topik Security Operations Centers. Beliau adalah instruktur senior di SANS Institute.



Sumber Pustaka

- SANS Course: Pen Testing Mobile Devices: <https://sans.org/sec575>
- SANS Course: Advanced Smartphone Forensics Course: <https://sans.org/for585>
- FTC Advice on Disposing Your Mobile Device: <https://www.consumer.ftc.gov/articles/0200-disposing-your-mobile-device>

OUCH! diterbitkan oleh SANS "Security Awareness" dan didistribusikan sesuai lisensi Creative Commons BY-NC-ND 4.0. Anda diperkenankan menyebarkan buletin ini atau menggunakannya di dalam program pembelajaran sejauh tidak melakukan perubahan isi buletin. Untuk keperluan alih bahasa atau informasi lainnya, silakan menghubungi www.sans.org/security-awareness/ouch-newsletter. Dewan Redaksi: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Diterjemahkan oleh: T. Gunawan