

# OUCH!

## DALAM ISU INI...

- Maklumat Anda
- Membersihkan Peranti Anda
- Kad SIM / Storan

## Melupuskan Peranti Mudah Alih Anda Secara Selamat

### Pengenalan

Peranti mudah alih, seperti telefon mudah alih, jam pintar dan tablet semakin maju dan kehadapan dengan amat pantas. Natijahnya, sesetengah orang menukar peranti mudah alih mereka sekerap setahun sekali. Malangnya ramai orang melupuskan peranti mereka tanpa memikirkan betapa banyak maklumat peribadi yang terdapat di dalamnya. Dalam surat berita ini kami akan mengupas jenis-jenis maklumat peribadi yang mungkin terdapat dalam peranti mudah alih anda dan bagaimana anda boleh membersihkannya sebelum melupus atau memulangkannya. Jika peranti mudah alih anda diberikan oleh majikan, atau mempunyai maklumat organisasi di dalamnya, pastikan anda memaklumkan penyelia untuk membuat sandaran dan pelupusan yang betul sebelum mengambil langkah seterusnya.

### Editor Jemputan

Heather Mahalik (@HeatherMahalik; +HMahalik) merupakan seorang Saintis Forensik Utama/Kanan yang mengetuai kerja-kerja forensik untuk ManTech CARD. Beliau merupakan ketua kursus dan penulis bersama untuk kursus Advanced Smartphone Forensics (FOR585) dan pengajar bagi Windows Forensic Analysis (FOR408) untuk SANS Institute. Beliau menulis blog di [smarterforensics.com](http://smarterforensics.com).

### Maklumat Anda

Peranti mudah alih menyimpan lebih banyak maklumat sensitif dari yang anda ketahui, malah selalunya lebih dari komputer anda. Maklumat yang biasa termasuklah

- Tempat anda tinggal, kerja dan selalu lawati
- Maklumat kenalan semua orang di dalam buku alamat dan aplikasi, termasuklah keluarga, sahabat, dan rakan sekerja
- Sejarah panggilan termasuklah keluar, masuk dan panggilan terlepas
- SMS (pesanan ringkas), pesanan suara dan multimedia
- Sesi bersembang di dalam aplikasi seperti komunikasi selamat, permainan dan media sosial
- Sejarah lokasi berdasarkan koordinat GPS atau sejarah menara sel
- Sejarah laman sesawang, sejarah carian, cookies dan simpanan laman
- Gambar peribadi, video, rakaman audio dan emel
- Kata laluan yang tersimpan dan capaian kepada akaun peribadi, seperti perbankan dalam talian atau e-mel
- Capaian kepada gambar, fail atau maklumat yang tersimpan di Awan
- Sebarang maklumat berkaitan kesihatan, termasuk umur, kadar degupan jantung, tekanan darah atau diet

### Membersihkan Peranti Anda

Seperti yang boleh anda lihat, terdapat kebarangkalian yang tinggi untuk peranti mudah alih anda menyimpan maklumat sensitif. Tidak kira bagaimana anda melupuskan peranti mudah alih anda, seperti mendermanya, menukarnya dengan yang

## Melupuskan Peranti Mudah Alih Anda Secara Selamat

baru, memberikan kepada ahli keluarga yang lain, menjualnya ataupun buang, anda perlu memastikan semua maklumat sensitif telah di padam. Anda mungkin tidak menyedari bahawa dengan hanya memadam adalah tidak memadai kerana, ia boleh dipulihkan dengan menggunakan alatan percuma yang boleh didapati di internet. Sebaliknya anda perlu memadam maklumat anda pada peranti itu dengan selamat, yang dinamakan peluputan. Perbuatan ini sebenarnya menulis semula maklumat untuk memastikan ianya tidak boleh dipulihkan. Ingat, sebelum anda membersihkan semua maklumat, anda mungkin mahu membuat sandaran dahulu, dengan cara ini anda boleh membina semula peranti baru anda dengan mudah.

Cara paling mudah untuk membersihkan peranti anda adalah dengan menggunakan fungsi 'tetapan semula kilang'. Ini akan menjadikan peranti anda kepada keadaan asal seperti anda baru membelinya. Kami mendapati tetapan semula kilang merupakan cara paling mudah dan selamat untuk memadam maklumat daripada peranti mudah alih anda. Tetapan semula kilang berbeza dari setiap peranti; senarai di bawah adalah langkah untuk dua peranti paling popular.

- Peranti iOS Apple: Settings | umum | Reset | Padam Semua Kandungan dan Tetapan
- Peranti Android: Aturan | Privasi | Aturan Semula Data Kilang

Malangnya, untuk memadam maklumat peribadi pada peranti telefon Windows tidak semudah tetapan semula kilang. Terdapat banyak penyelidikan untuk cara bagaimana untuk memastikan data peribadi anda di padam dari peranti. Jika anda masih tertanya-tanya tentang melakukan tetapan semula kilang, semak panduan pengguna atau laman sesawang pengeluar. Ingat, memadam maklumat peribadi anda tidak cukup kerana ianya boleh di pulihkan dengan mudah.

### Kad SIM & Storan

Selain dari maklumat yang tersimpan di dalam peranti anda, anda juga perlu mempertimbangkan apa yang perlu anda lakukan dengan kad SIM (Modul Identiti Pelanggan) anda. Peranti mudah alih menggunakan kad SIM untuk membuat sambungan selular dan data. Apabila anda membuat tetapan semula kilang, kad SIM masih menyimpan maklumat tentang akaun dan terikat dengan anda sebagai pengguna. Jika anda ingin menggunakan semula nombor yang sama dan bertukar kepada peranti yang baru, maklumkan kepada penyedia perkhidmatan untuk memindahkan kad SIM anda. Jika tidak boleh, sebagai contoh telefon baru anda menggunakan kad SIM yang berbeza saiz, simpan kad SIM lama anda dan lupuskannya secara fizikal untuk menghalang orang lain dari menggunakannya semula.



*Apabila melupuskan peranti anda, pastikan anda melakukan tetapan semula kilang dan keluarkan semua kad SIM dan SD yang terdapat di dalam peranti anda.*

## Melupuskan Peranti Mudah Alih Anda Secara Selamat

Akhir sekali, sesetengah peranti mudah alih menggunakan kad SD (Secure Digital) berasingan untuk storan tambahan. Kad storan ini selalunya mengandungi gambar, aplikasi telefon pintar dan kandungan sensitif yang lain. Pastikan anda mengeluarkan sebarang kad storan luaran dari peranti mudah alih anda sebelum melupuskannya (untuk sesetengah peranti, kad SD anda mungkin terselindung di dalam ruang bateri, berkemungkinan di bawah bateri). Kad ini selalunya boleh digunakan semula di dalam peranti baru anda, atau boleh digunakan sebagai storan biasa dengan menggunakan adaptor USB. Jika kad SD anda tidak boleh digunakan semula, kami mencadangkan anda melupuskannya secara fizikal.

Jika anda tidak pasti dengan mana-mana langkah yang dibincangkan dalam surat berita ini, bawa telefon mudah alih anda ke kedai anda membelinya dan dapatkan bantuan dari juruteknik yang terlatih. Akhirnya, jika anda ingin melupuskan peranti mudah alih anda, kami mencadangkan supaya anda pertimbangkan untuk mendermanya. Terdapat banyak organisasi amal yang menerima peranti mudah alih.

### 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 [securingthehuman.sans.org/ouch/archives](http://securingthehuman.sans.org/ouch/archives).

### 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

Securing Your New Tablet:	<a href="https://securingthehuman.sans.org/ouch/2016#january2016">https://securingthehuman.sans.org/ouch/2016#january2016</a>
Backup and Recovery:	<a href="https://securingthehuman.sans.org/ouch/2015#august2015">https://securingthehuman.sans.org/ouch/2015#august2015</a>
Advanced Smartphone Forensics Course:	<a href="https://sans.org/for585">https://sans.org/for585</a>
OUCH Newsletter Archives:	<a href="https://securingthehuman.sans.org/ouch/archives">https://securingthehuman.sans.org/ouch/archives</a>

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 mendedarkan 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, Cheryl Conley  
Translated by: Muhamad Hashimi, Rahayu Aziz, and Sheikh Ahmad Raffie



[securingthehuman.sans.org/blog](http://securingthehuman.sans.org/blog)



[/securethehuman](https://securethehuman)



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



[securingthehuman.sans.org/gplus](https://securingthehuman.sans.org/gplus)