

# OUCH!

## Dalam Edisi Ini...

- Sekilas
- Cara Kerja Pengelola Sandi
- Memilih Pengelola Sandi

## Pengelola Sandi

### Sekilas

Salah satu tindakan paling penting perlindungan diri di dunia online adalah menggunakan sandi unik untuk akun. Dalam prakteknya, setiap orang bisa saja memiliki banyak akun sehingga tidak jarang kerepotan mengingat beragam sandi yang dipakai. Persoalan itu bisa diatasi dengan menggunakan pengelola sandi (password manager) atau dikenal juga sebagai brankas sandi. Ini merupakan sebuah aplikasi yang dirancang untuk menyimpan data penting login Anda dengan aman. Selain itu, aplikasi ini akan memudahkan Anda dalam melakukan login ke situs web, aplikasi alkom dan lainnya.

### Editor Tamu

Leny Zeltser berfokus pada pengamanan sistem TI pelanggan di NCR Corp sekaligus melatih para ahli keamanan profesional di SANS Institute. Lenny aktif di Twitter sebagai [@lennyzeltser](https://twitter.com/lennyzeltser) serta menulis artikel di [zeltser.com](http://zeltser.com).

### Cara Kerja Pengelola Sandi

Pengelola sandi bekerja seperti layaknya brankas digital dan berfungsi sebagai tempat aman penyimpanan user-id, sandi dan informasi. Pada saat sebuah situs web meminta Anda untuk login, pengelola sandi akan menyiapkan sandi dan melakukan login ke situs web. Hal ini mempermudah penanganan banyak sandi karena Anda tidak perlu mengingatnya satu persatu lagi.

Pengelola sandi menyimpan rincian semua data di dalam database yang dikenal juga sebagai "vault". Pengelola sandi mengenkripsi isi vault serta melindunginya lagi dengan sandi yang Anda tentukan. Saat membutuhkan sebuah kredensial, sebagai misal untuk login ke jasa perbankan online atau akun surel, Anda cukup memasukkan sandi ke dalam pengelola sandi untuk membuka vault.

Beberapa pengelola sandi menyimpan vault di dalam sistem lokal atau alkom, ada pula yang disimpan di situs web dibawah pengelolaan produsen pengelola sandi. Selain itu, kebanyakan pengelola sandi sanggup melakukan proses sinkronisasi isi vault keberbagai peralatan yang Anda tentukan. Jadi bila terjadi perubahan sandi di laptop, perubahan itu akan ditularkan pula ke alkom, tablet atau komputer lain yang digunakan. Terlepas dimana database disimpan, Anda harus memasang aplikasi pengelola sandi di sistem atau peralatan dimana akan digunakan.

## Pengelola Sandi

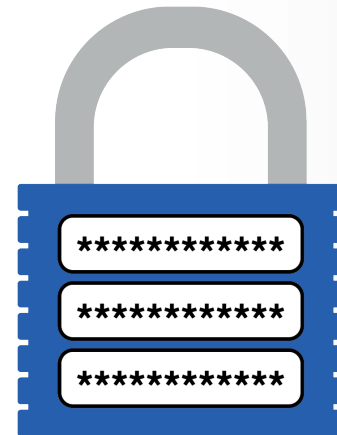
Pada saat menyiapkan pengelola sandi, setiap data login dan sandi harus dimasukkan satu persatu. Setelah itu, pengelola sandi akan bisa mendeteksi dan melakukan penyegaran data bila terjadi pembuatan akun online baru atau pengubahan sandi dari akun yang sudah ada. Hal ini dimungkinkan karena kebanyakan pengelola sandi berintegrasi dengan browser web. Integrasi inilah yang memungkinkan proses login otomatis ke situs web.

Pengelola Sandi dirancang untuk menyimpan data sensitif dengan aman. Karena itu sangatlah penting sandi utama yang dipakai untuk mengunci vault dibuat dengan benar dan sangat susah ditebak orang lain. Malahan sangat disarankan menggunakan frasa sandi untuk menjadikan sandi lebih kokoh. Bila sistem pengelola sandi mendukung proses verifikasi dua tahap, sebaiknya gunakan fasilitas itu. Ingat pula untuk tidak menggunakan sandi pengelola sandi di sistem atau akun lain. Dengan demikian, seandainya orang lain mendapat salinan sebuah vault, upaya menebak sandi dan mengakses isinya tidak akan berhasil. Satu hal lagi, pastikan tidak pernah lupa sandi utama pengelola sandi. Bila hal itu terjadi, akses ke semua sandi didalamnya tidak akan bisa dilakukan.

### Memilih Pengelola Sandi

Banyak pengelola sandi gratis dan berbayar yang bisa dipilih. Untuk menentukan mana yang paling cocok, ingat beberapa hal berikut ini:

- Pastikan pengelola sandi bisa berfungsi disemua sistem dan alkom yang memerlukan akses ke vault. Hal ini juga akan memudahkan proses sinkronisasi isi vault kesemua peralatan.
- Hanya gunakan pengelola sandi yang sudah dikenal dan terpercaya. Waspada terhadap produk-produk baru atau hanya mendapatkan sedikit ulasan. Seperti halnya anti-virus palsu, kriminalis siber bisa saja menciptakan pengelola sandi palsu justru untuk mencuri sandi.
- Pengelola sandi semestinya mudah digunakan. Bisa dirasa terlalu rumit, carilah produk lain yang lebih cocok.
- Pastikan apapun yang dipilih, selalu lakukan proses pembaruan dan penyempurnaan perangkat lunak serta gunakan versi terbaru.
- Pengelola sandi selayaknya mempermudah pengguna dalam memilih sandi yang kuat untuk berbagai akun,



*Pengelola Sandi adalah solusi mudah penyimpanan dan penggunaan beragam sandi Anda.*

## Pengelola Sandi

termasuk kemampuan mengusulkan sandi kuat sekaligus mengukur tingkat kekuatan sandi yang dipilih.

- Pengelola sandi harus memberikan pilihan untuk menyimpan data sensitif seperti jawaban pertanyaan rahasia keamanan, kartu kredit ataupun nomer Kartu Pelanggan Maskapai Penerbangan.
- Berhati-hati bila pengelola sandi menggunakan teknik enkripsi khusus dan tidak memakai metode enkripsi yang lazim dipakai. Bila metode enkripsi yang digunakan dirancang-bangun sendiri, hindari produk tersebut.
- Hindari pengelola sandi yang menyatakan bisa mendapatkan sandi utama saat dibutuhkan. Ini berarti sandi utama tidak lagi terjamin kerahasiaannya sehingga mengundang lebih banyak resiko.

Pengelola sandi merupakan solusi serbaguna dalam menyimpan berbagai sandi dan data sensitif. Lantaran pengelola sandi melindungi informasi penting, pastikan menggunakan sandi yang susah ditebak/dibobol pihak lain namun tetap mudah untuk diingat pemakainya.

### Selanjutnya

Untuk berlangganan buletin bulanan OUCH! Kesadaran Keamanan, mengakses arsip buletin OUCH! dan mengetahui lebih banyak solusi kesadaran keamanan SANS, silakan kunjungi <http://www.securingthehuman.org>.

### Versi Bahasa Indonesia

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

### Sumber Pustaka

Frasa Sandi:	<a href="http://www.securingthehuman.org/ouch/2015#april2015">http://www.securingthehuman.org/ouch/2015#april2015</a>
Verifikasi Dua Tahap:	<a href="https://www.securingthehuman.org/ouch/2015#september2015">https://www.securingthehuman.org/ouch/2015#september2015</a>
Top Five Password Managers:	<a href="http://lifehacker.com/5529133/five-best-password-managers">http://lifehacker.com/5529133/five-best-password-managers</a>
SANS Security Tip of the Day:	<a href="http://www.sans.org/tip_of_the_day.php">http://www.sans.org/tip_of_the_day.php</a>

OUCH! diterbitkan oleh SANS "Securing The Human" dan didistribusikan sesuai lisensi [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/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 [ouch@securingthehuman.org](mailto:ouch@securingthehuman.org).

Dewan Redaksi: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis  
Diterjemahkan oleh: T. Gunawan



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



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



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



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