

OUCH!

Dalam Edisi Ini...

- Frasa Sandi
- Aman Menggunakan Frasa Sandi
- Sumber Pustaka

Frasa Sandi

Latar Belakang

Sandi adalah sesuatu yang digunakan hampir setiap hari, mulai dari akses surel, perbankan online hingga berbelanja atau mengakses alkom (alat komunikasi multiguna/ smartphone). Namun, sandi juga mengusung banyak kelemahan; bila seseorang berhasil mendapatkan atau menebak sandi Anda, mereka akan bisa mengakses akun Anda, bahkan memindahkan dana, membaca surel atau mencuri identitas. Sandi yang kuat sangat penting untuk perlindungan. Dilain pihak, sandi bisa jadi memusingkan, sulit diingat dan diketik. Dalam edisi ini akan dibahas pembuatan frasa sandi, yakni sebuah sandi yang kokoh, mudah diingat serta gampang diketik.

Editor Tamu

My-Ngoc Nguyen (baca Me-Nop Wynn) adalah instruktur SANS bersertifikat sekaligus CEO/ Konsultan Utama di Secured IT Solutions. Beliau berbagi keahlian dari beragam sertifikasi dan telah lebih dari 14 tahun mengembangkan, mematangkan dan mengelola program keamanan di berbagai industri dan sektor. Twitter [@MenopN](#), LinkedIn: My-Ngoc "Menop" Nguyen.

Frasa Sandi

Peretas siber selalu mengembangkan metodi canggih dan efektif untuk menebak sebuah sandi. Dengan cara ini pihak yang tidak berkepentingan bisa meretas sandi yang tidak kokoh dan mudah ditebak. Langkah penting untuk mengatasi hal tersebut adalah dengan menggunakan sandi yang kuat. Biasanya dilakukan dengan memilih sandi yang rumit, tapi hal ini menjadikannya tidak mudah diingat, memusingkan dan sulit diketiknya. Untuk itu disarankan penggunaan frasa sandi, terdiri dari serangkaian kata atau sebuah kalimat. Semakin banyak karakter dalam sebuah frasa sandi, akan menjadikannya semakin kuat. Cara ini memudahkan dalam mengingat dan mengetik namun susah untuk diretas. Berikut adalah dua contoh untuk disimak:

Sustain-Easily-Imprison

Makan Siang Jam 1:23

Apa yang membuat frasa sandi tersebut kuat adalah bukan hanya panjangnya, namun digunakannya huruf besar dan simbol (ingat spasi dan tanda baca adalah simbol). Selain itu frasa sandi ini mudah diingat dan diketik. Frasa sandi diatas bisa

Frasa Sandi

diperkuat lagi dengan cara mengganti huruf dengan angka atau simbol, misalnya mengganti huruf 'a' dengan simbol '@' atau huruf 'o' dengan angka nol. Bila situs web atau program membatasi jumlah karakter yang bisa digunakan dalam sebuah sandi, buatlah sandi dengan panjang maksimal.

Aman Menggunakan Frasa Sandi

Anda wajib waspada dalam penggunaan frasa sandi. Frasa sandi yang mudah dicuri atau ditiru tentu tidak akan banyak bermanfaat.

1. Gunakan frasa sandi berbeda untuk setiap akun dan peralatan. Misal, jangan pernah menggunakan frasa sandi yang sama untuk urusan kerja/akun perbankan dengan akun pribadi di Facebook, Youtube atau Twitter. Dengan cara ini, bila salah satu akun diretas, akun lainnya tetap aman. Bisa ada terlalu banyak frasa sandi untuk diingat (lumrah terjadi), pertimbangkan menggunakan pengelola sandi. Ini adalah program khusus untuk menyimpan semua frasa sandi dengan aman. Anda hanya perlu mengingat satu frasa sandi untuk peralatan komputer atau peralatan dan pengelola sandi.
2. Jangan pernah berbagi frasa sandi atau strategi pembuatannya dengan orang lain, termasuk rekan kerja dan penyelia. Ingat, frasa sandi bersifat rahasia, bila pihak lain tahu frasa sandi Anda, menjadikannya tidak aman lagi. Bila tanpa sengaja sebuah frasa sandi terungkap, atau mencurigai frasa sandi diretas atau dicuri, ubahlah dengan segera. Perkecualian hanya dalam kondisi darurat, dimana Anda berbagi frasa sandi dengan anggota keluarga yang bisa dipercaya. Salah satu cara adalah dengan menuliskan frasa sandi (pastikan tidak berhubungan dengan kerja/bisnis), simpan ditempat aman dan beritahukan lokasi tersebut ke anggota keluarga yang bisa dipercaya. Bila terjadi kondisi darurat, anggota keluarga bisa mengakses akun penting tersebut.
3. Jangan gunakan komputer publik seperti di hotel atau cafe internet untuk mengakses akun Anda. Karena siapa saja bisa menggunakannya, bisa saja komputer tersebut sudah terinfeksi dan mencatat semua penggunaan papan ketik. Akses akun Anda hanya dari komputer atau alkom yang terpercaya.
4. Waspada situs web yang meminta jawaban atas pertanyaan yang bersifat pribadi. Pertanyaan ini biasanya dipakai bila Anda lupa frasa sandi dan perlu mengubahnya. Terkadang jawaban dari pertanyaan ini bisa ditemukan di internet atau bahkan dari laman Facebook Anda. Pastikan jawaban pertanyaan pribadi itu tidak diketahui orang lain atau gunakan



Frasa sandi merupakan cara lebih gampang untuk membuat dan mengingat sandi kuat.

Frasa Sandi

data fiktif buatan Anda. Tidak bisa mengingat semua jawaban pertanyaan pribadi itu? Pilih tema tertentu seperti karakter film dan buat pilihan jawaban Anda seputar karakter tersebut. Pilihan lain adalah menggunakan pengelola sandi lagi, banyak yang memberikan kemudahan untuk menyimpan informasi tambahan di dalamnya.

5. Berbagai akun online menawarkan otentifikasi dua faktor, dikenal juga sebagai otentifikasi dua tahap. Proses ini tidak hanya membutuhkan frasa sandi namun juga kode tertentu yang dikirimkan ke alkom. Cara ini lebih aman dari pada sekedar frasa sandi saja. Bila memungkinkan, gunakan fasilitas otentifikasi ini.
6. Alkom kebanyakan membutuhkan PIN untuk pengaman akses. Ingat, PIN sebenarnya adalah juga sandi. Semakin panjang PIN, semakin aman. Banyak alkom memungkinkan perubahan PIN menjadi frasa sandi atau biometrik seperti sidik jari.
7. Bila sebuah akun tidak lagi digunakan, pastikan untuk menutup, hapus atau menonaktifkannya.

Selanjutnya

Untuk berlangganan buletin bulanan OUCH! Kesadaran Keamanan, mengakses arsip buletin OUCH! dan mengetahui lebih banyak solusi kesadaran keamanan SANS, silakan kunjungi securingthehuman.sans.org/ouch/archives.

Versi Bahasa Indonesia

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

Daftar Pustaka

- Pengelola Sandi: <https://securingthehuman.sans.org/ouch/2015#october2015>
- Verifikasi dua tahap: <https://securingthehuman.sans.org/ouch/2015#september2015>
- Lock Down Your Login: <https://lockdownyourlogin.com>
- SANS SEC301 - Five day course on cyber security basics: <https://sans.org/sec301>

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.

Dewan Redaksi: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Diterjemahkan oleh: T. Gunawan

