Buletin Bulanan Keamanan Komputer

Menyederhanakan Sandi

Sekilas

Sering dikatakan bahwa sandi adalah faktor terpenting untuk melindungi akun (memang benar) namun jarang diterangkan kiat praktis membuat sandi dan tata-kelolanya. Di bawah ini ada tiga langkah mudah untuk menyederhanakan sandi, memproteksi semua akun dan melindungi masa depan Anda.

Frasa Sandi

Sekarang, kerumitan sebuah sandi bukanlah hal utama. Sandi yang rumit umumnya malah merepotkan, susah diingat, tidak mudah diketik dan gampang dijebol dengan bantuan komputer super cepat. Faktor terpenting sebuah sandi adalah panjangnya, semakin panjang rentengan karakternya, akan semakin baik. Ini dinamakan frasa-sandi, jenis sandi kuat dengan menggunakan kalimat pendek atau kata acak. Contohnya:

Waktunya minum Kopi!
bibit-bobot-bebet-babat

Dua sandi kuat diatas tersusun dari lebih 20 karakter, mudah diingat dan gampang diketik namun susah ditebak. Anda akan menemui situs web yang mengharuskan penggunaan simbol, angka atau huruf besar dalam sebuah sandi. Namun ingat, hal terpenting adalah panjang sandi.

Pengelola Sandi

Anda perlu sandi berbeda untuk setiap akun. Bila satu sandi yang sama digunakan dibeberapa akun, potensi resiko akan meningkat. Penyerang siber akan meretas situs web yang Anda gunakan, mencuri semua sandi termasuk milik Anda, kemudian menggunakan sandi itu untuk mengakses semua akun Anda. Sering kali hal ini terjadi tanpa disadari. Tidak percaya? Coba akses situs www.haveibeenpwned.com untuk memerikasa apakah akun dan sandi Anda pernah dibobol. Jadi bagaimana baiknya? Gunakan pengelola sandi.

Pengelola sandi adalah program khusus dirancang untuk menyimpan berbagai sandi secara terenkripsi. Anda hanya perlu mengingat satu sandi saja, yaitu sandi pengelola sandi. Progam ini akan secara otomatis memberikan sandi pada saat dibutuhkan dan mengakses situs web bagi Anda. Biasanya dilengkapi fitur untuk menyimpan jawaban pertanyaan rahasia, memastikan

Anda menggunakan sandi kuat, mencegah pengulangan penggunaan sandi dan fitur lainnya. Kebanyakan pengelola sandi ini akan melakukan sinkronisasi ke beragam komputer dan gawai, jadi apapun sistem yang digunakan, bakal memudahkan akses ke berbagai sandi milik Anda.

Selain itu, jangan lupa mencatat dengan baik sandi pengelola sandi dan menyimpannya di tempat aman di rumah. Beberapa pengelola sandi malah menyediakan fitur untuk mencetak panduan mereset pengelola sandi. Ini penting saat Anda lupa sandi pengelola sandi, atau dalam kondisi luar biasa (sakit berhalangan), pasangan atau keluarga bisa membantu mendapatkan informasi itu.

Verifikasi Dua Tahap

Verifikasi dua tahap (dikenal juga sebagai otentifikasi dua faktor atau otentifikasi multi faktor) bertujuan untuk memberikan perlindungan extra. Dengan metode ini, dibutuhkan dua hal sebagai syarat agar bisa login ke sebuah akun yaitu sandi dan sebuah kombinasi angka yang muncul di gawai atau telepon. Proses ini memastikan bila seseorang berhasil mendapatkan sandi, akun Anda tetap tidak akan bisa diakses. Verifikasi dua tahap mudah penerapannya, cuma perlu dipasang satu kali saja di setiap peralatan. Gunakan fitur ini bila mungkin, khususnya untuk melindungi akun penting seperti bank, pensiun atau surel (email). Bila Anda menggunakan pengelola sandi, sangat disarankan menggunakan frasa sandi dan juga verifikasi dua tahap.

Kelihatan sepele, namun tiga langkah sederhana diatas sangat penting dalam melindungi profesi, reputasi dan masa depan keuangan Anda.

Versi Bahasa Indonesia

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

Editor Tamu

Justin Henderson *(@SecurityMapper) adalah salah seorang pendiri H&A Security Solutions, Instruktur bersertifikat di SANS Institute dan perancang modul SANS Cyber Defense and SIEM. Beliau menyukai bidang cyber defense dan menjadi konsultan selama lebih dari 15 tahun.*

Sumber Pustaka

Have I Been Pwned:	https://haveibeenpwned.com/
Two-factor Authentication Site:	https://twofactorauth.org/
NIST SP800-63B Digital Identity Guidelines:	https://pages.nist.gov/800-63-3/sp800-63b.html
Poster: You Are a Target:	https://www.sans.org/u/OGi