Password: Pertahanan tingkat pertama

Berapa banyak password yang kamu punya?
Bagaimana caramu mengingat semuanya tanpa harus menuliskannya?
Apakah kamu enggan mengubah password karena takut lupa?
Apakah kamu menggunakan satu password untuk semuanya?

Password (kata sandi) yang aman masih menjadi bagian penting dalam melindungi informasimu baik online maupun offline. Dengan berkembangnya layanan online dan jejaring sosial, ada lebih banyak kesempatan untuk menggunakan *password*.

Sekarang, informasi yang berkaitan denganmu tidak lagi hanya ada dalam komputer dan perangkat penyimpanan personal milikmu, tetapi juga di web (melalui layanan internet seperti Google Mail, atau Facebook). Oleh karena itu, informasi tentangmu berada dalam jaringan (*online*) dan sangat terbuka bagi serangan kejahatan internet.

- Apakah kamu ingat kapan terakhir kali mengubah *password*?
- Apakah kamu memiliki *password* yang sama setidaknya pada 2 layanan di Internet?
- Apakah kamu pernah menggunakan lagi *password* lama?
- Apakah kamu pernah menggunakan satu *password* bersama?
- Apakah *password* kamu berisi kata-kata umum yang terdapat dalam kamus dan/atau informasi umum tentang diri kamu (nama kerabat, tanggal lahir, alamat dan sejenisnya)?
- Apakah *password* kamu terdiri atas 8 karakter atau kurang?
- Apakah kamu pernah menuliskan *password* di selembar kertas?
- Apakah kamu pernah mengakses layanan online melalui warnet dan kamu tidak begitu yakin bahwa warnet tersebut mempunyai jaminan keamanan dan privasi yang baik?

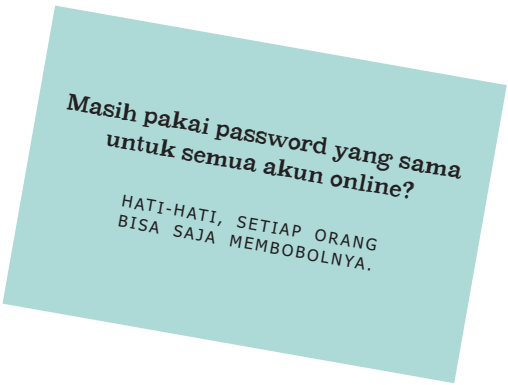
Tips/ solusi:

- Semakin panjang *password* akan semakin baik. *Password* sebaiknya lebih panjang dari 12 karakter (misal: heer-izlw/12).
- Untuk membuatnya aman, acak kata atau ganti kata dengan k@rakt3r atau nom3r khusus. Cobalah gunakan frasa sandi (*passphrase*) sebagai *password*. Frasa sandi dapat berupa judul buku (misal: va dinci kode), atau kutipan dari sebuah lagu.

- *Password* bisa mengandung huruf BESAR dan huruf kecil, nom3r, dan k@rakt3r khusus. Jika dimungkinkan (oleh sistem dan/atau layanan online) *password* bisa mengandung spasi.
- *Password* mestinya tidak menggunakan kata-kata umum yang terdapat dalam kamus dan/atau informasi umum tentang dirimu, seperti nomor telepon, nama binatang peliharaan, alamat, dan sejenisnya.
- Sering-seringlah mengganti *password*.
- Jangan gunakan *password* yang sama pada akun atau layanan internet yang berbeda.
- Jangan tulis *password*, cukup simpan mereka dalam ingatanmu selama memungkinkan (kamu juga dapat menggunakan *password* yang dikelola *software*).
- JANGAN PERNAH berbagi *password*.
- JANGAN PERNAH izinkan *website* dan program menyimpan *password*mu.
- Verifikasi keamanan warnet sebelum kamu mengakses layanan online.

Butuh bantuan soal password? Kamu bisa klik :

https://keepass.info/
https://keepassx.org/

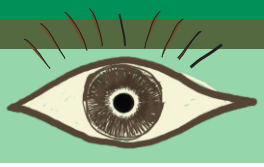


TACTICAL TECHNOLOGY COLLECTIVE

Front Line
PROTECTION OF HUMAN RIGHTS DEFENDERS

Lihat juga perangkat kami : **securityinabox.org/id**

Edisi bahasa Indonesia ini diterjemahkan dan dicetak oleh Combine Resource Institution
www.combine.or.id
Yogyakarta, Maret 2018



Berjejaring sosial dengan aman

Boleh jadi perangkat dan layanan jejaring sosial adalah layanan terpopuler di internet dewasa ini. Jejaring sosial menghubungkan kita dengan lingkaran pertemanan maupun teman potensial, lebih daripada sebelumnya. Perangkat dan layanan ini memungkinkan kita berbagi informasi dalam bentuk pesan, gambar, berkas (*files*) dan lokasi. Informasi tersebut dapat dibagikan secara aktual (*real-time*) ataupun disimpan untuk kemudian diakses saat kita membuka akun jejaring sosial kita.

Jejaring sosial juga dimanfaatkan oleh perusahaan dan organisasi, serta digunakan secara efektif oleh berbagai kelompok advokasi untuk berkampanye. Jelas sekali bahwa jejaring sosial akan mengambil peran penting untuk jangka panjang, sebab ketika semakin banyak orang terhubung, semakin banyak pula layanan yang akan disediakan.

Kekhawatiran terkait privasi dan keamanan perangkat dan jaringan ini juga terus meningkat, seiring maraknya berita tentang pencurian identitas dan informasi yang mengakibatkan kerugian finansial, reputasi bahkan kerusakan fisik. Jika kita berurusan dengan informasi dan topik sensitif, penting untuk mengenal lebih dekat masalah privasi dan keamanan seputar jejaring sosial.

Panduan berikut akan membantu melindungi kita dan orang lain, serta menentukan apakah keuntungan penggunaan jejaring sosial lebih banyak daripada implikasi keamanan jangka panjang maupun jangka pendeknya.

Ketidakamanan jejaring sosial

- Kebanyakan jejaring sosial:
  - Memungkinkan kita menggunakan layanan mereka secara gratis namun mungkin meminta kita untuk menyerahkan informasi milik kita. hanya
  - Menyediakan nama pengguna (*username*) dan *password* sebagai sebuah syarat keamanan untuk menjaga identitas dan informasi kita dari pihak yang tidak berwenang (*unauthorised access*).
  - Hanya dapat diakses melalui *browser* yang mempunyai kerentanan dan ketidakamanan tersendiri.
  - Diakses melalui internet yang membuatnya rentan akan semua ancaman dan serangan di internet.

- Berbagi informasi merupakan fitur bawaan (*default)* dan dapat dengan mudah terabaikan apabila kita tidak mengetahui pengaturan privasinya.
- Jejaring sosial memiliki cara yang berbeda dalam melindungi atau membuka informasi kita.
- Kita tidak punya kendali atas aktivitas teman yang membagikan informasi tentang kita. Mereka bisa saja membagikan gambar, lokasi dan informasi lainnya yang mungkin secara tidak sengaja membahayakan privasi dan keamananan kia.

Hal-hal yang perlu dipertimbangkan

- Baca dan pahami Perjanjian Lisensi Pengguna (*End User License Agreement* [EULA]), dokumen ketentuan penggunaan (*Terms of Use*) dan/atau paduan privasi (*Privacy Guidlines*). Sebagian besar jejaring sosial mempunyai setidaknya salah satu dari dokumen tersebut. Dokumen tersebut dapat berubah sewaktu-waktu, sehingga sangat penting meninjaunya kembali secara berkala.
- Pastikan telah mengetahui dengan baik pengaturan privasi akun jejaring sosial yang akan digunakan. Jangan mengandalkan pengaturan bawaan, aturlah sendiri agar dapat mengontrol informasinya. Tinjau pengaturan secara rutin untuk mengantisipasi perubahan kebijakan layanan berkala.
- Hati-hati saat memasang aplikasi yang disarankan oleh layanan jejaring sosial. Gunakan aplikasi tersebut hanya jika bisa mempercayai sumbernya, memahami informasi apa saja yang akan mereka buka, dan apa saja yang dapat mengendalikan arus keluar informasi kita.
- Pikirkan dengan cermat mengenai informasi orang lain yang kita bagikan.
- Mintalah persetujuan jika akan mengunggah informasi, dokumen, gambar dan lokasi orang lain.
- Pastikan *password* aman dan diganti secara berkala.
- Hati-hati saat mengakses akun jejaring sosial di layanan internet publik (misalnya: wi-fi di tempat umum). Warnet merupakan salah satu tempat yang umum didatangi untuk mengakses jejaring sosial, namun gunakanlah hanya jika benar-benar mempercayainya.
- Hapus *password* dan riwayat penjelajahan setelah mengunakan browser atau komputer

Bahan bacaan lebih lanjut :

https://www.eff.org/deeplinks/2010/04/facebook-timeline

https://www.eff.org/deeplinks/2010/06/encrypt-web-https-everywhere-firefox-extension

TACTICAL TECHNOLOGY COLLECTIVE

Front Line
PROTECTION OF HUMAN RIGHTS DEFENDERS

Lihat juga perangkat kami : **securityinabox.org/id**

Edisi bahasa Indonesia ini diterjemahkan dan dicetak oleh Combine Resource Institution
www.combine.or.id
Yogyakarta, Maret 2018

Keamanan telepon seluler

Telepon genggam atau ponsel digunakan oleh individu, kelompok dan banyak organisasi di berbagai tempat. Sejumlah kelompok masyarakat sipil menggunakan teknologi ponsel dengan cara baru dan kreatif: untuk peringatan dini bencana, layanan kesehatan, pemantauan pemilu, dan banyak lagi. Sebagian besar ponsel juga telah dilengkapi dengan layanan internet. Kamu mungkin bisa menggunakan ponselmu untuk berselancar (*browsing*), mengirim e-mail maupun layanan internet lainnya (meskipun layanan ini masih terbatas pada ponsel-ponsel canggih, yang umumnya lebih mahal), tergantung pada ponsel yang kamu gunakan.

Ketidakamanan

Ponselmu dan informasimu

Telepon genggam atau ponsel digunakan oleh individu, kelompok dan banyak organisasi di berbagai tempat. Sejumlah kelompok masyarakat sipil menggunakan teknologi ponsel dengan cara baru dan kreatif: untuk peringatan dini bencana, layanan kesehatan, pemantauan pemilu, dan banyak lagi. Sebagian besar ponsel juga telah dilengkapi dengan layanan internet. Kamu mungkin bisa menggunakan ponselmu untuk berselancar (*browsing*), mengirim e-mail maupun layanan internet lainnya (meskipun layanan ini masih terbatas pada ponsel-ponsel canggih, yang umumnya lebih mahal), tergantung pada ponsel yang kamu gunakan.

Sebagian besar ponsel menghimpun banyak informasi tentang dirimu, menyimpannya dalam kartu SIM, memori telepon, bahkan beberapa ponsel canggih dapat menyimpannya dalam kartu memori eksternal. Kamu akan mengakses informasi dengan mengendalikan menu pada ponsel. Stuktur menu yang rumit di kebanyakan ponsel bisa membuatmu tidak sadar telah meninggalkan informasi sensitif di suatu tempat di ponselmu.

Sayangnya, kebanyakan ponsel tidak membolehkanmu untuk menghapus informasi yang tidak diinginkan atau sensitif dengan sekali hapus. Sebagai contoh, untuk menghapus sebuah kontak person, kamu harus membuka buku telepon, sementara untuk menghapus pesan (SMS atau MMS) kamu harus masuk ke menu *pesan keluar* atau *pesan masuk*.

Sekarang ini, sebagian besar ponsel tidak mengenkripsi informasimu (padahal itu cara terbaik melindungi privasi); tawaran terbaik mereka justru penggunaan *password* untuk membuka atau mengunci informasi ponselmu.

Pesan singkat (SMS) dan panggilan suara (voice calls)

Pengaturan dan teknologi ponsel saat ini (termasuk *SMS* dan *voice calls*) tidaklah aman. Penyedia layanan menyimpan informasi penggunaan ponsel, seperti: tanggal, waktu, lokasi, penerima, pengirim, lokasi, panjang SMS, durasi panggilan dan akses internet (jika ada).

Informasi ini biasanya digunakan untuk menentukan tagihan (jumlah pulsa yang harus dikeluarkan) sekaligus dapat digunakan untuk melemahkan keamanan dan privasimu, teman serta kolega-kolegamu. Pesan SMS juga dapat dengan mudah disimpan ketika pesan tersebut keluar dan masuk.

SMS dan pesan suara cenderung mudah disadap. Pesan SMS dikirim dan diterima dalam bentuk teks sederhana (*plain text*), artinya siapapun dapat membacanya selama mereka dapat mengakses ponselmu, begitu pula saat pesan

sedang dikirim. Maka, bukan hanya penyedia layanan ponsel yang dapat melihat SMSmu, tapi juga siapa pun yang dapat menyadap jaringan seluler karena pesan-pesan tersebut melintasi jaringan seluler dalam rupa teks sederhana.

Lokasimu

Agar berfungsi dengan baik, ponsel akan terus terhubung dengan menara sinyal yang berada di sekitarnya untuk memastikan ke mana harus mengirim panggilan teleponmu. Ketika kamu menghidupkan ponsel, salah satu hal pertama yang dilakukannya adalah mencari sinyal dari penyedia layanan. Menara dengan sinyal terbaik dan terdekat biasanya akan langsung mendaftarkan ponselmu ke dalam sistemnya sehingga segala bentuk komunikasi dari dan untukmu akan dilakukan lewat menara ini.

Saat kamu bergerak, kamu bisa jadi terhubung dengan menara yang berbeda dan lokasimu secara otomatis akan diperbaharui oleh sistem. Dengan demikian, sepanjang ponselmu menyala, ia akan memberitahukan perkiraan lokasi ke jaringan penyedia layanan. Pergerakanmu juga meninggalkan jejak karena (sinyal) ponselmu "dialihkan" dari menara satu ke menara lain. Akibatnya, penyedia layanan dapat melacakmu (dan ponselmu) sehingga dia dapat mengarahkan panggilan maupun SMS yang keluar dan masuk.

Hal-hal yang perlu diperhatikan

- Aktifkan *password* atau kunci pin ponselmu.
- Jangan simpan informasi sensitif di ponselmu, atau jika memang kamu harus melakukannya, samarkan informasi tersebut sehingga hanya kamu yang memahaminya.
- Hapuslah informasi yang tidak diinginkan dan/atau sensitif secara rutin.
- Selalu waspada dengan lingkungan sekitar saat kamu mengeluarkan dan menggunakan ponsel, dan jangan gunakan ponselmu di tempat atau situasi yang berisiko.
- Pastikan semua informasimu sudah terhapus dari ponsel sebelum menjualnya atau memperbaikinya.
- Hancurkan ponsel dan kartu SIM yang sudah tidak dapat digunakan sebelum membuangnya.
- Pikirkan baik-baik sebelum menggunakan ponsel untuk mengirim informasi sensitif. Adakah cara lain yang lebih aman?
- Ketika bekerja dengan orang ataupun organisasi yang berurusan dengan informasi sensitif, pertimbangkan untuk memakai ponsel dan kartu SIM berbeda untuk pekerjaan dan pribadi.

TACTICAL TECHNOLOGY COLLECTIVE

Front Line
PROTECTION OF HUMAN RIGHTS DEFENDERS

Lihat juga perangkat kami : **securityinabox.org/id**

Edisi bahasa Indonesia ini diterjemahkan dan dicetak oleh Combine Resource Institution
www.combine.or.id
Yogyakarta, Maret 2018

Mengamankan email

Kita lebih terhubung dari sebelumnya dengan internet. Kita dapat mengirim pesan berisi 140 karakter (dengan Twitter), *ngobrol* online (dengan Google-talk), membuat panggilan (dengan Skype) atau berbagi foto dan video.

Kendati demikian, email tetap menjadi media komunikasi utama kita di internet, baik untuk kepentingan personal maupun pekerjaan. Oleh karena itu, mari kita perhatikan keamanan (atau kelemahan) email dan keamanan informasi kita di internet. Ketika kita berpindah dari satu kota ke kota lain, maka keamanan kita akan terbagi menjadi : keamanan di tempat asal, keamanan di tempat tujuan, keamanan di jalan, dan keamanan diri sendiri sebagai pejalan (*traveller*). Pada email berbasis web, penyedia layanan email bisa kita anggap sebagai "tempat asal", adapun bagian antarmuka email (*email interface*) bisa kita anggap sebagai "tempat tujuan", transmisi internet (transmisi: proses pengiriman data dari salah satu sumber data ke penerima data menggunakan komputer/media elektronik) sebagai "jalan", dan konten email sebagai "pejalan/traveler".

Penyedia layanan : penjaga informasimu

Pada tahun 2007 terjadi peningkatan layanan *free email* (email gratis) dan tren tersebut terus berlanjut. Ini artinya, akses untuk berkirim pesan melalui email menjadi lebih mudah (bahkan bagi mereka yang tidak memiliki komputer atau akses internet reguler), dan ruang penyimpanan online menjadi semakin besar. Ini juga berarti risiko menjadi semakin tinggi karena adanya tarik menarik antara kemudahan akses dengan pengendalian data kita. Perhatikan hal-hal berikut saat menggunakan layanan email gratis:

- Informasimu (email, lampiran, dll.) berada di server penyedia layanan. Tidak banyak yang kita ketahui tentang bagaimana mereka beroperasi, kita terpaksa memercayakan informasi kita dan orang-orang yang berkomunikasi dengan kita kepada mereka.
- Pahamilah apa yang diinginkan penyedia layanan dan bagaimana mereka menggunakan informasi kita (bacalah sebelum mengklik tombol 'saya setuju [I agree]'…).
- Untuk email dan komunikasi yang lebih sensitif, pertimbangkan untuk menggunakan layanan email gratis yang menjamin secara jelas bahwa mereka akan melindungi dan tidak akan menggunakan/membocorkan informasi kita (misalnya: baca di securityinabox.org/id/guide/riseup/web/
- Komunikasi adalah proses dua arah. Pastikan orang yang berkomunikasi dengan kita juga menggunakan layanan yang aman. Email kita tidak akan terlindungi jika hanya satu pihak saja yang menggunakan layanan email yang aman.

Interface : bagaimana mengakses emailmu

Cara paling sering digunakan untuk mengakses email adalah melalui peramban web (*web browser*). Setiap orang dapat dengan mudah masuk ke email melalui web tanpa perlu komputer dan internet reguler. Mengakses email dengan cara ini artinya informasi akan melintas dari server (tempat informasi kamu disimpan) ke kamu (melalui browser).

Browser (seperti internet explorer atau Firefox) sangat rentan terhadap serangan kejahatan di internet. Jadi ketika menggunakan browser untuk membaca dan mengirim pesan, kita sebetulnya sedang meningkatkan potensi risiko membeberkan informasi pada orang lain.

Pertimbangkanlah memakai browser yang lebih aman. Firefox adalah pilihan yang baik dan lebih aman lagi jika kamu menginstal *add-ons* (pengaya) keamanan dan privasi. Baca lebih lengkap di https://securityinabox.org/id/guide/firefox/linux/
https://securityinabox.org/id/guide/firefox/windows/

Transmisi : bagaimana email kita bergerak

Mengamankan informasi di kedua ujung (*ends*), yakni di tempat asal dan tujuan pesan, *bisa* memberi sejumlah perlindungan. Sebab, jalur di antara dua ujung (*ends*) tersebut sama pentingnya. Biasanya, email bergerak di antara server email dan kita (pengguna) dengan keamanan terbatas atau tidak ada keamanan sama sekali. Pesan email kita biasanya dikirimkan dalam bentuk teks sederhana (*plain text*). Artinya siapapun yang memiliki akses ke jalur transmisi dapat membaca pesan email kita. Coba perhatikan hal-hal berikut:

- Saat menggunakan layanan email gratis, cek URL kita (kolom alamat pada browser). Jika alamat dimulai dengan http, maka transmisi kita tidak aman dan email kita akan terkirim dalam bentuk teks sederhana.
- Beberapa email berbasis web (misalnya, Yahoo! Mail) menyediakan keamanan hanya ketika mentransmisikan password kita (selama *log in*), sementara yang lainnya (misalnya, Google Mail) menyediakan https untuk keseluruhan interaksi dalam layanan.

Konten : Pesan aktual

Pada akhirnya, hal yang kita upayakan agar tetap terjaga dan tidak terekpos adalah isi pesanmu. Dengan kata lain, tidak ada seorangpun yang diberikan izin melihat/mengakses informasi didalamnya saat pesan tersebut melakukan perjalanan dari kamu ke server penyedia layanan, ataupun dalam perjalanan ke penerima pesan, namun:

- Begitu kita mengirimkan email, kita tidak mempunyai kontrol atas email itu lagi. Jika orang yang berkomunikasi dengan kita tidak sadar keamanan, email kita dan keamanan (yang kita upayakan) bisa jadi sia-sia.
- Jika kita menyimpan email dalam komputer pribadi, orang lain yang mungkin memiliki akses ke komputer tersebut tetap dapat membacanya.

Solusi untuk permasalahan ini adalah dengan enkripsi yang merupakan salah satu cara terbaik untuk melindungi isi email, berkas ataupun informasi sensitif. Mengenkripsi informasi berarti kita menulis pesan dalam bentuk sandi atau mengacaknya dengan bantuan alat (dan kunci untuk membuat dan membuka sandi), dan pesan itu hanya bisa terbaca saat kita membuka sandi atau memberikan kunci untuk membukanya.

TACTICAL TECHNOLOGY COLLECTIVE

Front Line
PROTECTION OF HUMAN RIGHTS DEFENDERS

Lihat juga perangkat kami : **securityinabox.org/id**

Edisi bahasa Indonesia ini diterjemahkan dan dicetak oleh Combine Resource Institution
www.combine.or.id
Yogyakarta, Maret 2018