

Waspadai Pembajakan Akun Facebook Anda

By: M. Salahuddien* & Sam Ardi**

Beberapa hari ini media memberitakan tentang pencurian password akun facebook user di beberapa tempat baik di Indonesia maupun luar negeri. Para korban mengaku setelah log out terakhir kali dan keesokan harinya mencoba log in ternyata gagal mengakses dengan beberapa alasan seperti “password dan username tidak cocok” ataupun “akun tidak eksis”. Di beberapa social networking lainnya, seperti twitter dan plurk sempat dilaporkan kejadian yang sama pernah terjadi. Username dan password tiba-tiba tidak cocok dikarenakan sesuatu hal, atau dapat kita ambil benang merah, password mereka ada yang mengganti.

Apakah ada suatu teknik cracking untuk membobol akun facebook antar individu? Jawabannya ada beberapa. Lalu pertanyaan selanjutnya adalah, apakah ada teknik untuk melumpuhkan akun facebook atau social networking lainnya. Teknik yang terungkap untuk menyerang akun facebook beberapa waktu lalu adalah dengan membanjiri data pada server facebook dengan teknik DDOS atau biasa dikenal dengan *Distributed Denial of Service* sehingga server lumpuh selama beberapa jam seperti yang terjadi pada facebook dan twitter tahun 2009 oleh cracker dari Rusia. Kemungkinan seperti ini perlu kita waspadai.

Keylogger

Cara pertama menggunakan keylogger adalah cara yang sangat efektif bagi para cracker untuk mencuri password dari akun facebook anda. Dengan menginstall software dan atau hardware keylogger pada notebook maupun PC sasaran, maka otomatis segala bentuk ketukan pada keyboard maupun aktifitas browsing anda akan terekam dengan detail dan sistematis. Sehingga jika anda mengetikan password dan username pada notebook atau PC yang telah dipasang keylogger, anda dengan penuh kerelaan hati telah menyerahkan data pribadi sensitif tersebut pada orang yang memasangnya, karena keylogger ibarat kertas karbon yang akan membuat salinan tentang sesuatu yang ditulis di atasnya.

Keylogger biasanya dipasang oleh cracker pada terminal akses internet publik yang berbagi pakai seperti di warnet dan kampus. Maka berhati-hatilah ketika menggunakan akses seperti ini. Pertama, jangan langsung menggunakan terminal melainkan lakukan restart. Kedua, coba cek apakah ada aplikasi tersembunyi yang berjalan di memori background, anda bisa gunakan tools event task manager (tekan tombol ctrl + alt + del pada desktop windows anda) dan perhatikan apakah ada aplikasi atau proses yang tidak biasa? Memang anda perlu sedikit belajar dan membiasakan hal ini demi keamanan anda sendiri. Ketiga, cek setting keamanan pada browser yang anda gunakan apakah secara otomatis merekam username dan password? Sebaiknya matikan fitur ini dan apabila ada fitur anti phishing site bisa diaktifkan. Keempat, bersihkan/hapus cache dan history secara otomatis setiap kali menutup browser. Ini bisa anda lakukan pada setting browser. Kelima, pastikan bahwa setiap selesai melakukan kegiatan anda selalu log out dengan sempurna.

Sniffing

Teknik kedua adalah dengan menggunakan tools yang biasa digunakan sniffing seperti Cain and Abel pada area yang terkoneksi WiFi jadi tools tersebut memang “mencari aktifitas” pada laptop-laptop yang terkoneksi. Maka anda harus berhati-hati juga apabila sedang mobile dan mengakses HotSpot. Pada prinsipnya akses wireless sangat mudah untuk diintip. Jangan begitu saja mempercayai SSID “Free WiFi atau Free HotSpot” saat anda scanning wireless network. Yang paling aman adalah bertanya pada pengelola HotSpot area tersebut apa SSID yang resmi? Kemudian setting akses wireless pada notebook anda untuk tidak “auto connect” melainkan harus manual agar anda bisa meneliti terlebih dahulu.

Ketika anda melakukan akses dari jaringan WiFi HotSpot sebaiknya hindarkan transaksi pada situs yang kritis seperti e-banking, akses email, akun jejaring sosial dlsb. Browsing hal yang umum saja kecuali anda yakin benar bahwa tidak ada yang berusaha mengintip aktivitas anda dan jaringan tersebut bisa dipercaya. Meskipun demikian, pastikan bahwa anda selalu akses dengan memilih mode secure connection yaitu menggunakan HTTPS yang biasanya ditandai dengan munculnya icon gembok terkunci pada browser anda. Dengan akses HTTPS ini maka antara anda dengan server layanan yang diakses telah dilindungi dengan enkripsi sehingga tidak mudah diintip oleh orang yang tidak berhak. Pastikan anda sudah masuk ke mode secure sebelum memasukkan username dan password atau PIN.

Phising

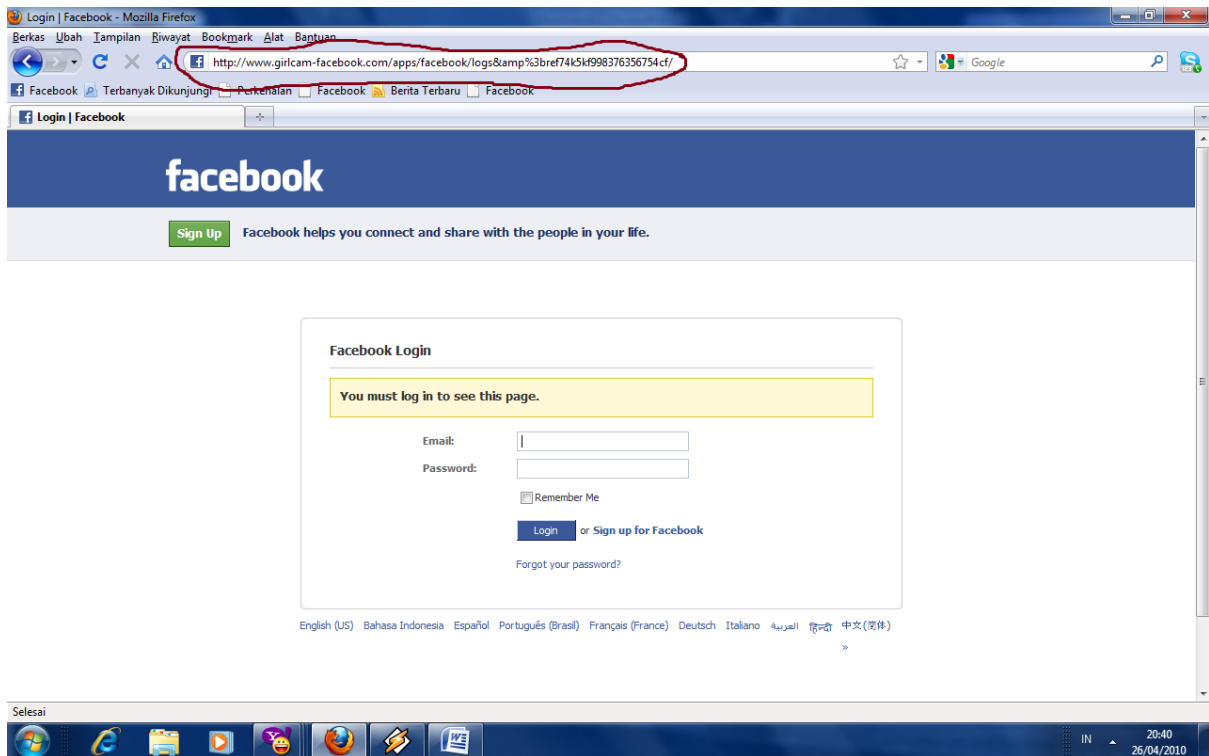
Cara ketiga adalah dengan mengklik url yang diberikan oleh aplikasi facebook maupun via email yang mengatasnamakan facebook. Atau menjebak anda dengan tawaran aplikasi asing pada facebook merupakan aplikasi yang lepas dari maintenance facebook sendiri. Aplikasi tersebut dapat dibuat oleh siapa saja dan kapan saja dan random sifatnya. Untuk mencuri username dan password tersebut, biasanya korban disuruh mengakses link tersebut dan diperintahkan memberikan password dan usernamena. Perhatikan contoh berikut:

Contoh 1:

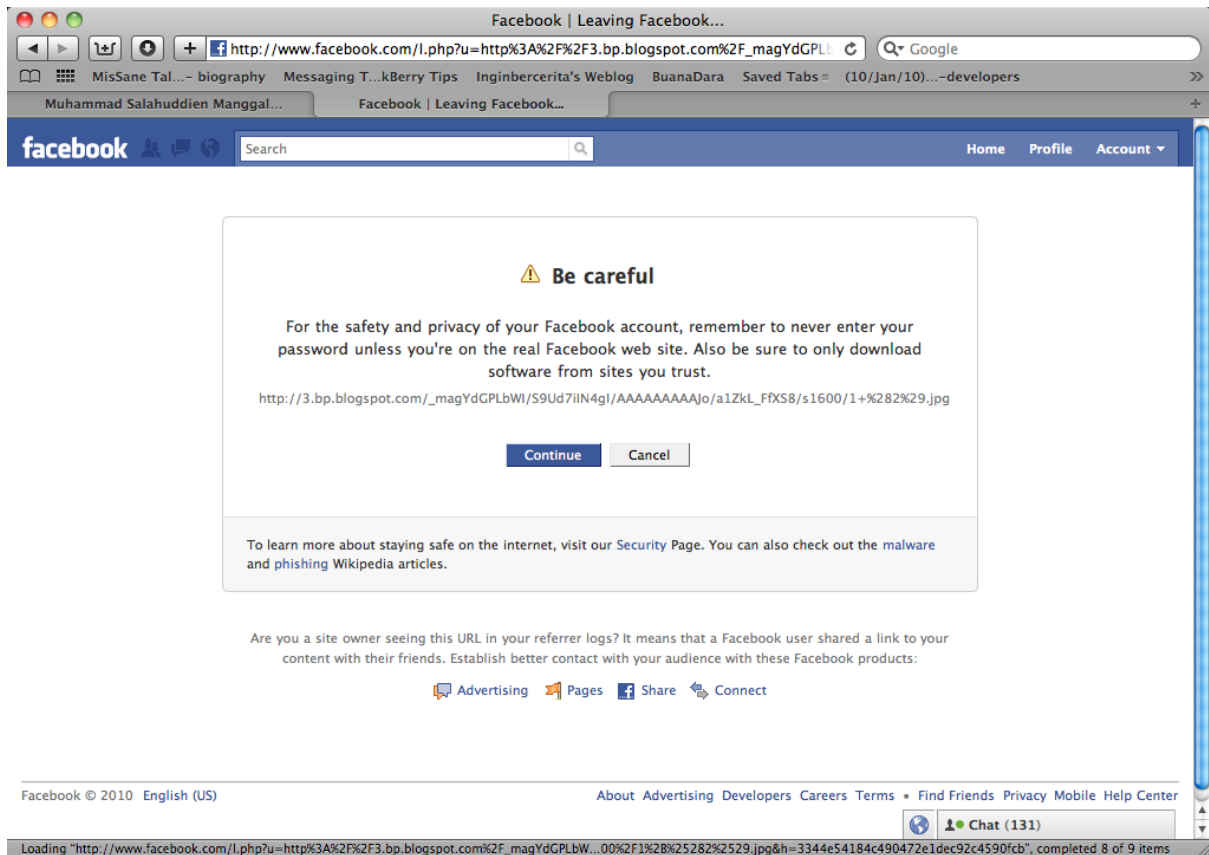
Anda diminta untuk mengakses link tertentu:

<http://www.facebook.com/l.php?u=http%3A%2F%2Fwww.girlcam-facebook.com%2Fapps%2Ffacebook%2Fbookmark%2526amp%253bcode2432kn4khkh34&h=f2a5c924ad5de97a77f440ac31753781>

Namun ketika anda mengkliknya anda harus log in dahulu di halaman tersebut, padahal anda sebelumnya sudah log ini terlebih dahulu. Jangan pernah anda masukan username ataupun password jika anda menemui hal janggal seperti ini, karena dapat diindikasikan hal tersebut adalah phising dengan menggunakan fake log in facebook, perhatikan screenshot di bawah:



Ada sesuatu yang janggal, anda sudah log in sebelumnya dan ketika anda mengakses link diatas anda disuruh log in kedua kalinya. Jelas ini adalah bentuk phishing di mana sang pencuri password menipu anda dengan mendesain halaman “orisinil” dari facebook. Perhatikan dengan baik-baik url pada kolom tempat anda memasukan url, agar tidak menjadi korban. Dan perhatikan apabila anda mendapatkan peringatan dari facebook semacam ini:



munculnya halaman peringatan facebook ini menandakan bahwa anda sebenarnya sedang mengakses situs (url) lain di luar web site resmi facebook, sehingga anda perlu berhati-hati dan jangan pernah memberikan apabila diminta memasukkan ulang username dan password atau jangan pernah melakukan bila diminta mendownload suatu software, program, aplikasi atau dokumen tertentu yang sekilas nampaknya berguna atau menarik (misalnya games, tools dlsb.) karena bisa jadi itu sebenarnya adalah malware.

Masalahnya adalah, kebanyakan pengguna facebook kurang memperhatikan pesan peringatan seperti ini, tidak membaca isinya atau karena kurang memahami maksudnya dan kendala bahasa dan mengabaikannya. Perlu dibiasakan, apabila menjumpai hal yang tidak biasa atau meragukan bahkan anda tidak mengerti apa maksudnya, maka tindakan paling aman adalah selalu menolak dan memilih klik tombol “cancel”. Atau langsung tutup halaman tersebut, sampai anda mendapatkan keterangan yang terpecaya.

Contoh 2:

Dahulu ada sebuah group di dalam facebook yang memberikan teknik untuk mengambil password akun orang lain dengan alamat tersebut:

<http://www.facebook.com/group.php?gid=202000763768>

Kemudian kita lihat apa yang tertera pada halaman group “Cara Mengetahui Password Teman Anda” tersebut:

1 KLIK "Join this Group" ATAU "Gabung ke Grup Ini"
(hanya anda yang telah bergabung yang bisa menggunakan fasilitas ini!)

2 KLIK "Invite People to Join" ATAU "Undang Orang untuk Bergabung"

3 CENTANG Semua teman anda, minimal 100 orang agar bisa berjalan!
(hanya teman anda yang telah di undang yang bisa anda lihat segala aktivitasnya di facebook anda!)

4 KLIK Tombol "Send Invitations" ATAU "Kirim Undangan"

kirim pesan ke admin facebook dengan mengcopy link :

<http://www.facebook.com/home.php?#/i....3256059163..1>

KEMUDIAN kirim pesan dengan petunjuk berikut:

**.gx=0&.tm=1259467892&.rand=fnvrijkff2bk4e |(ALAMAT EMAIL
ANDA)/config/login?.src=fpctx&.intl=us&.done=http%3A%2F%2Fm(PAS SWORD EMAIL
ANDA) | 202000763768&ref=nf##hl=id&source=hp&q=/7601524/id/f#id(ALAMAT EMAIL YANG
AKAN ANDA KETAHUI PASSWORDNYA)**

klik send email

kemudian dengan menunggu konfirmasi balasan dari facebook admin dalam waktu 24jam, anda akan mendapat email balasan dan mengetahui password facebook teman anda.

=====

Perhatikan kalimat yang cetak tebal tersebut, ada sesuatu yang ganjil bukan? Anda ingin mengetahui password orang lain tetapi anda sebelumnya disuruh memasukan password dan username anda terlebih dahulu. Jelas ini merupakan upaya jebakan terhadap akun anda. Harus selalu diingat bahwa username dan password adalah sesuatu yang vital, sama seperti PIN ATM biarlah anda, pihak bank dan Tuhan saja yang mengetahuinya. Jangan pernah berikan kepada pihak lain, apapun alasannya termasuk permintaan dari seseorang yang mengaku sebagai admin. Sebab kalau benar dia adalah admin, tentu tidak memerlukan username serta password anda untuk melakukan maintenance atau tindakan apapun.

Terakhir, selalu ketikkan langsung alamat url situs pada jendela browser anda. Sebab ada juga malware yang menambahkan link bookmark sehingga anda mengira bahwa itu resmi padahal adalah penyesatan (phising). Malware yang lebih canggih bahkan bisa merubah informasi di etc/host yang memetakan alamat url secara statik pada komputer anda tanpa menggunakan mesin DNS. Sehingga ketika anda mengetikkan alamat jejaring sosial ternyata diarahkan ke phising site. Karena itu sangat penting untuk selalu waspada dan memeriksa keabsahan suatu url dan mengetahui adanya ketidakwajaran walaupun agak sulit.

Social Engineering

Sekarang ini mulai banyak korban berjatuh akibat upaya pembajakan akun facebook yang menggunakan teknik social engineering. Terutama memanfaatkan kelemahan prosedur akun email gratisan seperti Yahoo! Mail. Seseorang atau cracker bisa berpura-pura menjadi anda dan mencoba mendapatkan akses tidak sah dan membajak akun email anda. Caranya dengan mengikuti prosedur kehilangan password. Biasanya layanan email gratisan akan menanyakan beberapa kata kunci untuk konfirmasi seperti kombinasi “di mana tempat bulan madu anda?” atau “siapa nama hewan peliharaan anda yang pertama” atau “siapa nama paman atau tante yang jadi favorit anda?”. Jawaban atau kata kunci dari pertanyaan konfirmasi seperti ini dulu pernah anda isikan ketika pertama kali mendaftarkan akun email tersebut.

Sekarang melalui facebook, seseorang atau cracker bisa dengan mudah mengelabui anda. Dia akan berpura-pura melamar sebagai teman anda. Kemudian mencari tahu alamat email anda. Ketika dia mengetahui bahwa anda menggunakan alamat email gratisan, maka mulailah dia mengajak anda berkomunikasi. Dengan cara tertentu dia akan mengorek sejumlah informasi yang seharusnya anda rahasiakan. Begitu anda memberikan informasi yang diperlukan untuk mengakses prosedur kehilangan password di layanan akun email gratisan, maka si cracker akan menguasai akun email anda. Selanjutnya dia akan melakukan prosedur yang sama kepada akun facebook anda, yaitu pura-pura lupa password dan mencoba membajaknya. Facebook biasanya akan mengirimkan email “password sementara” ke alamat email utama anda yang sialnya sudah dikuasai oleh si cracker. Sehingga dengan mudah dia menguasai akun facebook anda juga. Begitu dia mengganti password akun facebook anda, maka selanjutnya anda akan ditolak untuk mengakses akun facebook anda sendiri.

Seorang cracker yang membajak akun facebook anda biasanya akan memanfaatkannya untuk beberapa tujuan jahat. Yang pertama adalah untuk melakukan impersonating atau pemalsuan identitas dengan maksud untuk memfitnah, menjelek-jelekan dan menjatuhkan martabat anda sebagai pemilik akun yang sesungguhnya. Misalnya dia menyerang dan melakukan suatu tindakan yang tidak disukai teman-teman anda sehingga di dunia nyata, semua orang menjadi memusuhi anda tanpa anda sadari. Yang kedua adalah untuk menipu teman-teman anda. Telah banyak laporan di luar negeri maupun juga di Indonesia, bahwa sejumlah orang dimintai tolong oleh teman lamanya di facebook untuk mengirimkan sejumlah uang karena beberapa alasan, yang klasik adalah mengaku kecopetan atau kerampokan atau di akhir pekan tidak bisa mengambil uang untuk pengobatan dsb. Atau mengajak bertransaksi sesuatu tapi sebenarnya akun facebook itu telah dibajak oleh orang lain.

1. Jangan mudah menerima permintaan pertemanan dari orang yang sama sekali belum anda kenal, terutama yang tidak memiliki mutual friend.
2. Anda selalu memiliki kesempatan untuk melakukan konfirmasi kepada teman yang ada di dalam mutual friend seseorang yang mencoba meminta pertemanan pada anda. Sebab memang itulah salah satu gunanya facebook menampilkan informasi mutual friend yaitu agar anda bisa melakukan verifikasi terlebih dahulu. Apabila teman anda

mereferensikan dan mengkonfirmasi keabsahan calon teman tersebut baru “lamaran” tersebut bisa dipertimbangkan untuk diterima.

3. Cara lain untuk mengkonfirmasi suatu permintaan pertemanan adalah mengirimkan message kepada yang bersangkutan. Dengan komunikasi ini anda dapat menanyakan siapakah dia sebenarnya (seringkali nama akun yang ditampilkan adalah julukan atau nama alias yang tidak membantu anda untuk mengingat siapakah calon teman itu) dan melakukan konfirmasi lainnya yang diperlukan. Misalnya, melakukan komunikasi off line (telepon) atau pertemuan on line web cam atau bahkan off line adalah cara lain untuk melakukan konfirmasi keabsahan calon teman.
4. Jangan terburu-buru dan berhati-hati dalam menyampaikan sejumlah informasi pribadi yang sekilas nampaknya tidak penting tetapi ternyata merupakan kunci untuk membobol akun email anda. Pertanyaan yang sepertinya menunjukkan antusiasme pada satu hal yang sama (binatang kesayangan, tempat wisata favorite, cerita tentang keluarga, memasang album foto event tertentu dlsb.) tanpa sengaja bisa memaparkan informasi pribadi yang seharusnya anda rahasiakan.
5. Anda mungkin tanpa sadar telah memaparkan informasi yang seharusnya rahasia itu dalam profile anda. Atau dalam words caption di album foto anda. Misalnya menulis nama binatang kesayangan anda persis di bawah fotonya bahkan ada orang yang secara khusus membuatkan akun facebook untuk binatang kesayangannya lengkap dengan semua profilnya. Atau memasang foto dan menyebut lokasi bulan madu dan atau memberikan tagging pada foto keluarga (termasuk paman yang menjadi favorite anda) dlsb. Beragam ketidaksengajaan semacam itu.
6. Berhati-hati dan pikirkanlah berkali-kali kemungkinan manfaat dan kerugiannya bila anda harus menampilkan informasi pribadi di halaman info akun facebook anda. Anda punya pilihan untuk tidak menuliskan informasi itu, misalnya binatang kesayangan, toh sebenarnya apabila ada yang ingin tahu, bisa menanyakannya secara pribadi melalui fasilitas message langsung kepada anda. Anda juga bisa memilih setting untuk membatasi akses orang lain ke informasi tertentu di akun facebook anda. Misalnya anda bisa menyembunyikan alamat email. Manfaatkan fitur setting pengamanan akun facebook ini semaksimal mungkin dan pikirkanlah.
7. Sebisa mungkin dan jikalau memungkinkan hindari menggunakan layanan email tak berbayar untuk akun facebook anda. Gunakanlah akun email lokal misalnya yang diberikan oleh kantor anda (kalau diijinkan untuk pribadi), menyewa akun email ke ISP (sebenarnya harganya murah atau bahkan gratis apabila anda menjadi pelanggan ISP tersebut) atau anda membuat domain pribadi sendiri dan meminta tolong layanan jasa hosting untuk membuatkan, apabila anda tidak memiliki keterampilan teknis sendiri. Intinya, akun email lokal atau milik sendiri lebih aman dari teknik serangan social engineering ini terutama karena prosedur untuk konfirmasi kehilangan password atau bila terjadi compromise biasanya dilakukan secara manual dengan

teknik identifikasi off line bukan by system yang otomatis tapi menggunakan algoritma pengamanan yang terlalu sederhana seperti layanan email gratisan.

8. Selalu tambahkan alamat email sekunder pada akun facebook anda dan juga pada akun email gratisan yang anda gunakan apabila memang terpaksa tidak ada pilihan selain harus menggunakan layanan tersebut. Sembunyikan atau jangan pernah anda tunjukkan kepada siapapun dengan alasan apapun alamat email sekunder anda itu. Dan secara periodik ubahlah semua password anda sesuai anjuran pengamanan seperti menggunakan kombinasi huruf, angka dan karakter khusus serta panjang password minimal 6 atau 8 karakter yang sulit ditebak orang lain dan bila sulit menghapalnya jangan simpan catatannya di tempat yang mudah diketahui. Atau gunakan fasilitas aplikasi password management untuk membantu anda. Ada banyak yang gratis.
9. Meskipun tidak lazim, namun demi untuk keamanan, backuplah data friend list anda. Informasi penting seperti nama profile accountnya, url halaman facebooknya, alamat email dan juga telepon (kalau ada). Sehingga apabila terjadi sesuatu anda bisa segera memberikan peringatan, misalnya melalui email dan akan berguna apabila kelak anda membuka akun facebook yang baru dan terpaksa harus memasukkan satu per satu lagi friend list anda tersebut. Backup memang sedikit merepotkan namun penting.
10. Apabila anda terlanjur menjadi korban pembajakan akun facebook maka anda dapat melakukan 4 hal. Pertama, peringatkan semua orang bahwa akun anda telah dibajak. Upaya ini bisa anda lakukan lewat berbagai saluran seperti email, telepon, milis, chat, blog dlsb. Demi untuk mencegah orang lain, teman, famili anda yang ada di friend list menjadi korban misalnya penipuan.
11. Kedua, patut secepatnya (anda berlomba dengan si pembajak sebelum dia mengganti alamat email utama dan sekunder anda) mencoba untuk mendapatkan kembali akun anda melalui prosedur lupa atau kehilangan password. Apabila berhasil, segera ganti alamat email anda dan passwordnya dan sembunyikan jangan ditampilkan dengan mengubah setting keamanan akun anda. Jangan buru-buru log out untuk mencegah si pembajak mencoba mengambil alih juga. Dan jangan log out sampai anda berhasil mengganti alamat email utama dan sekunder anda serta mengisi password yang baru sekaligus menerapkan setting pengamanan yang lebih tertutup (melindungi/sembunyikan alamat email anda).
12. Ketiga, melaporkan kepada tim keamanan facebook bahwa akun anda telah dibajak, alamatnya adalah: <http://www.facebook.com/help/?page=1023> atau apabila link tersebut telah berubah anda dapat mencarinya di halaman HELP. Anda akan diminta mengisi form dan selanjutnya akan ada korespondensi dengan tim keamanan facebook yang akan berusaha mengkonfirmasi kebenaran laporan anda dan apabila semua berjalan dengan baik, mungkin akun anda dapat dikembalikan. Namun pastikan bahwa sebelum melaporkan, anda sudah memiliki alamat email yang baru dan aman.
13. Yang keempat, apabila semua upaya mengembalikan akun anda gagal, maka segeralah membuka akun facebook baru, amankan informasinya agar tidak dibajak orang lagi

dan add semua teman anda (semoga anda melakukan back up). Kemudian bersama-sama ajaklah mereka semuanya untuk melaporkan akun lama anda yang dibajak tsb. Sebagai akun yang melakukan abuse, fraud, compromise dan impersonating sehingga nanti akan ditutup atau diblokir oleh facebook.

Yang terakhir jangan gunakan alamat email, username dan password yang sama untuk semua layanan online yang anda ikuti. Selalu update pengetahuan anda mengenai isu keamanan layanan jejaring sosial dan senantiasa waspada ketika aktif di dunia maya.

**Wakil Ketua ID-SIRTII (Indonesia Security Incident Response Team on Internet Infrastructure)*

***Pemerhati Cyber Law dan Cybercrime, ketua Bloggerngalam (Komunitas Blogger Kota Malang)*