MENJAGA AKUN *FB* ANDA[*)]

Enam tahu lalu situs jejaring sosial *FB* mulai diluncurkan di negara asalnya. *FB* mendapat respon luar biasa dari masyarakat pengguna internet dari segala lapisan sosial. Situs jejaraing sosial yang satu ini mampu menggeser populeritas situs jejaring sosial pendahulunya seperti twitter, friendster dan lain sebagainya. Meskipun tidak sampai menghilangkan pendahulunya, populeritas *FB* melesat jauh meninggalkan pendahulunya. Di Indonesia *FB* mulai dikenal dua tahun dan mendapat respon luar biasa dari masyarakat segala lapisan sosial dan lapisan umur. Segmen pengguna *FB* paling banyak pada usia remaja dan dewasa muda (18-24 tahun) dan diikuti oleh segmen umur 13-14 tahun. Populeritas *FB* tidak lepas dari keunggulan yang dimiliki *FB* yang memberikan kemudahan dan fasilitas lebih dari pendahulunya.

Pemanfaatan *FB* sangat beragam dari sekedar untuk mencari teman lama yang terpisah jarak sampai pemanfaatan untuk bisnis. Pemanfaatan biasanya dengan cara membuat jaringan pertemanan dengan mencari teman menggunakan e-mail, sekolah, pekerjaan atau nama. Cara kedua adalah dengan membuat grup. Cara inilah yang dimanfaatkan oleh komunitas tertentu untuk mencari dukungan seperti yen terjadi beberapa saat yang lalu untuk menggalang dukungan terhadap ketua KPK Bibit-Samad dan dukungan terhadap Prita Mulyasari. Cara ini sangat efektif untuk beberapa kasus. Grup *FB* juga dapat dimanfaatkan untuk menjalin komunitas bisnis seperti yang dilakukan oleh komunitas bisnis di Jepara. Meskipun demikian, *FB* juga dapat dimanfaatkan oleh pihak-pihak tertentu untuk melakukan kejahatan. Beberapa kasus kejahatan dengan memanfaatkan *FB* seperti penipuan, pelacuran online, pencemaran nama baik, dan penyalahguanan akun orang lain untuk melakukan kejahatan juga marak terjadi akhir-akhir ini. Pertanyaan yang muncul adalah bagaimana cara kita melindungi diri dari efek negatif tersebut? Amankah akun *FB* kita?

Sebelum kita membahas bagaimana kemanan dari *FB*, akan lebih baik kita pahami dahulu cara kerja dari *FB*. Perlu kita pahami bersama bahwa *FB* merupakan ruang virtual untuk bertemu satu orang dengan orang lain secara virtual. Ketika kita membuat akun baru di dalam *FB* secara otomatis kita mempunyai ruang pribadi yang tidak bisa diakses oleh orang lain selain diri sendiri. Tetapi ketika kita mencari teman dan teman tersebut menerima anda sebagai teman atau kita menerima ajakan pertemuan orang lain yang datang pada akun kita, maka secara otomatis ruang

yang kita miliki menjadi bisa diakses oleh teman kita yang tergabung dalam jaringan yang sama dengan kita jika kita mengijinkan. Hal tersebut dapat terjadi karena teman kita dapat mengakses “wall”, “profil” dan lain sebagianya dari akun kita selama kita mengijinkan. Atau dapat kita analogikan sebagai berikut: ada satu ruang besar (*FB*) didalamnya terdapat lima ruang yaitu ruang A,B,C,D, dan E. Ketika kita mendaftar untuk tinggal diruang besar tersebut kita diberi ruang A oleh pengelola ruang besar Pada suatu ketika penghuni ruang B yang memiliki teman penghuni ruang C, dan D mengajak anda berteman dan anda menerimanya, maka baik penghuni ruang B,C dan D dapat melihat isi ruang anda jika anda mengijinkan. Bagaimana penghuni ruang E? penghuni ruang E dapat melihat ruang anda dengan ketika diajak atau mengajak pertemanan dan diterima oleh anda (penghuni ruang A), penghuni ruang D,C, atau D. Dengan analogi tersebut maka *FB* dapat menjadi ruang virtual semi publik.

Dengan cara kerja tersebut maka isu keamanan menjadi sangat krusial dalam pemanfaatan *FB.* Seacara umum semua jenis sistem informasi memiliki dua sisi metoda pengamanan yaitu pengamanan secara teknis dan pengamanan secara manusia. Pengamanan secara teknis mengacu pada pengamanan yang bersifat teknikal sedangkan pengamanan sisi manusia mengacu pada perilaku pengguna dari sistem itu sendiri. Pengamanan teknis secara umum dapat dibagi menjadi dua yaitu pengamanan yang berupa pengamanan secara fisik dan pengamanan secara aplikasi. Pengamanan fisik dapat dilakukan dengan pembatasan akses terhadap sistem itu sendiri dengan cara fisik misalnya dengan meletakkan komputer pada ruang terkunci yang dijaga atau melepas jaringan internet dengan mencabut modem atau kabel jaringan. Tipe pengamanan fisik biasanya sulit diterapkan pada pengamanan *FB* karena jika akses suatu komputer dibatasi *FB* tetap dapat diakses menggunakan komputer lain.

Pengamanan teknis secara umum yang sering digunakan dalam faceebok adalah tipe pengamanan aplikasi. Tipe pengamanan aplikasi dilakukan dengan menambah fitur pengamanan terhadap aplikasi itu sendiri misalnya menggunakan *password* dan pengaturan setting keamanan. *Password* yang kita buat ketika kita membuat akun *FB* menjadi sangat penting untuk dirahasiakan. Sebagai tanggung jawab kepada penggunanya pihak penyelangara situs *FB* dapat dipastikan memberikan pengamanan pada situsnya dengan aplikasi yang layak. Fasilitas link untuk melaporkan penyalahguanan akun merupakan bukti nyata usaha pengamanan oleh

pengelola *FB*. Meskipun demikian usaha orang yang tidak bertanggungjawab tidak terhenti. Beberapa teknik seperti hacking, cracking, sniffing, dan lain sebagainya masih mungkin dilakukan. Aplikasi untuk melakukan hal tersebut banyak tersedia di pasar dengan harga relatif murah.

Pengamanan yang paling efektif dan mudah dilakukan bagi pengguna *FB* adalah pengamanan sisi manusia. Pengamanan sisi manusia adalah pengamanan yang berfokus pada manusia sebagai pengguna itu sendiri dalam konteks ini adalah pengguna *FB*. Pengguna *FB* harus memahami cara kerja *FB* dengan benar pemahaman tersebut dapat membantu pengguna *FB* untuk mengamankan diri dari ulah orang tidak bertanggungjawab. Beberapa tips dari, penulis yang dapat dilakukan sebagai berikut:

- Jangan biarkan komputer atau *browser* internet mengingat/merekam *password* untuk username anda. Jangan beri tanda centang pada kotak "*keep me login*" ketika anda ingin *login* dalam akun anda. Jika anda lakukan maka akun anda akan tetap terbuka jika anda menutup *browser*. Di samping itu, ketika kita memasuki suatu alamat web yang membutuhkan username dan *password* biasanya *browser* (misal *Firefox*) akan memberi kita konfirmasi agar komputer menyimpan *password* untuk username situs yang bersangkutan. Ketika konfirmasi itu muncul sebaiknya kita jawab tidak terutama jika kita mengakses *FB* dari tempat umum seperti warnet.
- Pastikan anda telah keluar (*logout*) secara benar dan sempurna sebelum meninggalkan komputer. Jangan langsung tutup *browser* sebelum. Beberapa *browser* internet akan melakukan *recovery* jika terjadi masalah dalam menjalankan program. Memastikan komputer sebelum menutup *browser* atau menutup *browser* tanpa *logout* terlebih dahulu terkadang dianggap sistem error dan *browser* akan melakukan *recovery* secara otomatis.
- Pastikan *history* komputer terhapus ketika meninggalkan *FB*. Lakukan setting pada *browser* anda untuk menghapus *history* ketika *browser* ditutup. File *history* dapat diakses oleh orang tertentu yang memahami sistem komputer dan terkadang *password FB* kita tercatat dalam file tersebut
- Jangan gunakan tanggal lahir, nama hewan peliharaan, nama anda, nama saudara, orangtua, pacar, kesukaan dan hal-hal pribadi yang mudah ditebak sebagai *password*.

Hal-hal tersebut mudah ditebak oleh orang lain. Kombinasi huruf dan angka merupakan *password* yang paling kuat.

- Kelola profil anda dengan baik. Profil anda merupakan data pribadi anda, data tersebut dapat memberikan manfaat tapi juga dapat dimanfaatkan oleh orang-orang yang tidak bertanggungjawab untuk melakukan kejahatan pada diri anda. *FB* memberikan kita fitur untuk membatasi siapa saja yang dapat melihat profil kita
- Maksimalkan fitur keamanan dalam *FB* dengan mengelola setting akun dengan maksimal. *FB* telah memberikan fitur keamanan dalam aplikasi anda. Jika dikelola denga baik *FB* maka akun *FB* anda relatif lebih aman.
- Hati-hati pada pesan yang mencurigakan. Pesan mecurigakan dapat berupa tawarkan sesuatu, tawarkan utuk melihat video, mengikuti link dan lain sebagainya. Tawarkan tersebut dapat menggiring kita pada situs tertentu atau bahkan berupa spam yang merugikan. Link mencurigakan dapat juga mengandung virus. Jangan langsung klik pesan mecurigakan, pelajari dahulu, baru putuskan.
- Tetaplah selektif memilih teman. Jika nada belum pernah kenal dan bertemu secara fisik dengan teman yang mengajak berteman melalui *FB* sebaiknya anda berhati-hati. Sikap kehati-hatian perlu dilakukan mengingat identitas yang digunakan dalam *FB* dapat dengan mudah dipalsukan.

Pengamanan paling baik adalah pengamanan yang dilakukan oleh pengguna *FB* itu sendiri. Perlu kita ingat bahwa *FB* dapat menjadi pisau bermata dua. Jika kita tidak hati-hati menggunakanya akan mencelakai kita sendiri. Dengan sifat *FB* dapat menjadi ruang virtual semi publik maka etika pergaulan umum akan tetap berlaku. Kasus pencemaran nama baik menggunakan *FB* dapat terjadi karena pengguna kurang bijaksana menggunakan *FB* dan melanggar etika pergaulan secara umum. Bagaimanapun juga *FB* hanya alat baik buruknya tergantung penggunanya. Ambil positifnya tingalkan negatifnya.

*) Diterbitkan pada harian Kedaulatan Rakyat 15 Maret 2010 halaman 15