PERTEMUAN VI

ETIKA BERINTERNET

A. Perkembangan Dunia Internet

Internet merupakan kepanjangan dari Interconection Networking atau juga telah menjadi International Networking merupakan suatu jaringan yang menghubungkan komputer di seluruh dunia.

Internet pertama kali dikembangkan oleh salah satu lembaga riset di Amerika Serikat, yaitu DARPA (Defence Advanced Research Projects Agency) pada tahun 1973. Pada saat itu DARPA membangun Interconection Networking sebagai sarana untuk menghubungkan beberapa jenis jaringan paket data seperti CS-net, BIT-net, NSF-net, dll.

Tahun 1972, jaringan komputer yang pertama dihasilkan adalah ARPnet yang telah menghubungkan 40 titik dengan menggunakan FTP. Pada perkembangannya titik yang dihubungkan semakin banyak sehingga NCP tak lagi dapat menampung, lalu ditemukan TCP dan IP.

Tahun 1984, host berkembang menjadi DNS dan tahun 1990 terdapat penambahan aplikasi diantaranya www, wais dan ghoper.

Dari segi penggunaan internetpun mengalami perkembangan mulai dari aplikasi sederhana seperti chatting hingga penggunaan VOIP.

Beberapa alasan mengapa internet memberikan dampak besar dalam segala aspek kehidupan :

a. Informasi di Internet dapat diakses 24 jam
b. Biaya relatif murah dan bahkan gratis
c. Kemudahan akses informasi dalam melakukan transaksi
d. Kemudahan membangun relasi dengan pelanggan

e. Materi dapat di update dengan mudah
f. Pengguna internet telah merambah ke segala penjuru dunia.

Karakteristik dunia maya (menurut Dysson, 1994) :

a. Beroperasi secara virtual/maya
b. Dunia cyber selalu berubah dengan cepat
c. Dunia maya tidak mengenal batas-batas teritorial
d. Orang-orang yang hidup dalam dunia maya dapat melaksanakan aktivitasnya tanpa menunjukkan identitas
e. Informasi didalamnya bersifat publik

B. Pentingnya Etika di Dunia Maya

Perkembangan internet yang begitu pesat menuntut dibuatnya aturan-aturan atau etika beraktivitas didalamnya. Berikut ini adalah beberapa alasan pentingnya etika dalam dunia maya :

a. Pengguna internet berasal dari berbagai negara yang memiliki budaya, bahasa dan adat istiadat yang berbeda
b. Pengguna internet merupakan orang yang hidupdalam anonymous, yang mengharuskan pernyataan identitas asli dalam berinteraksi
c. Bermacam fasilitas di internet memungkinkan seseorang untuk bertindak etis / tidak etis
d. Harus diperhatikan bahwa pengguna internet akan selalu bertambah setiap saat yang memungkinkan masuknya ‘penghuni’ baru. Untuk itu mereka perlu diberi petunjuk agar memahami budaya internet.

C. Contoh Etika Berinternet

Netiket atau Nettiquette, adalah etika dalam berkomunikasi menggunakan internet yang ditetapkan oleh IETF (The Internet Enginnering Task Force). IETF adalah sebuah komunitas masyarakat internasional yang terdiri dari para perancang jaringan, operator, penjual dan peneliti yang terkait dengan evolusi arsitektur dan pengoperasian internet.

Berikut salah satu contoh etika yang telah ditetapkan oleh IETF : Netiket One to One Communication adalah kondisi dimana komunikasi terjadi antar individu dalam sebuah dialog. Contoh komunikasi via email. Hal-hal yang dilarang :

a. Jangan terlalu banyak mengutip
b. Perlakukan email secara pribadi
c. Hati-hati dalam menggunakan huruf kapital
d. Jangan membicarakan orang lain
e. Jangan menggunakan CC (carbon copy)
f. Jangan gunakan format HTML
g. Jawablah secara masuk akal

D. Tips Aman Berinternet

Bijak dalam memBerikaN data pribadi di Medsos

Peraturan Perlindungan Data Pribadi (PDP) RI hingga saat ini masih dalam pembahasan, seperti PP 82/2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE). Institusi atau Perusahaan yang mengelola data base pribadi konsumen atau pengguna yang biasa disebut Data Controller disingkat menjadi DCO. DCO bertanggung jawab melindungi Data Pribadi Konsumen sebagai pemilik data. Setiap perlakuan terhadap Data dari seorang klien harus diberikan secara bebas atau berdasarkan keinginan atau tanpa tekanan dengan kata lain harus dengan persetujuan dan ijin dari klien pemilik Data.

Seorang pengguna sosmed, website atau konsumen ecommerce (Data Subject) memiliki hak privasinya:

1. Agar Data Pribadi (Personal) dihapus (delete) atau diremajakan (up to date);
2. Agar Data Pribadi (Privasi) dilindungi kerahasiaannya seperti informasi yang dapat mengidentifikasi (identifier): Nama, nomor ID, lokasi data, atau identifikasi dari faktor seperti fisik, genetik, mental, agama, sosial, budaya dan ekonomi seseorang
3. Agar perekaman, pengambaran dan analisa atas profile suatu objek harus seijin (consent) Data Subjek tersebut termasuk segala bentuk personalisasi, prediksi mengenai kinerja, pekerjaan, ekonomi, keuangan, kesehatan, referensi personal, interest, hobby, kelakuan, lokasi dan pergerakannya.

Tip Akutabilitas Perusahaan (DCO) Menjaga Data Pribadi Konsumen atau Masyarakat:

1. DCO wajib menjaga Keamanan terhadap Pembocoran Data Pribadi (Data Breach). Jika terjadi musibah pembocoran data harus segera melaporkan dalam waktu 72 jam setelah mengetahui (discovery).
2. DCO memproses data konsumen dengan cara Sah, tidak melanggar hukum, fair (adil) dan transparan terhadap konsumen untuk tujuan spesifik, jelas/eksplisit, valid & sah, sesuai dengan tujuan yang sudah disepakati oleh konsumen.
3. DCO menjamin ketepatan, akurasi data konsumen, tidak kadaluwarsa, up to date terus diperbarui, sesuai tujuan penyimpanan data yang disetujui oleh konsumen.
4. DCO menjamin Lokasi & format penyimpanan atau database disetujui konsumen dan UU yang berlaku.
5. DCO menjaga integritas (tidak rusak dan hilang) data dan kerahasian (confidentiality) data subjek dengan enkripsi, password dll.

Penggunaan Enkripsi Untuk Menjaga Integritas Data

Enkripsi (Encryption) adalahsuatu proses untuk merahasiakan berita agar pihak yang tidak berwenang tidak dapat membaca dan mengerti isi berita. Sebuah konversi dari tulisan yang bisa dibaca manusia (plain text) menjadi tulisan yang diacak (cypher text) menggunakan kunci (key). Namun enkripsi dapat dikembalikan dengan dekripsi (decryption) ke tulisan original (plain text) menggunakan kunci (key).

Kriptanalisis (Cryptanalysis) adalah suatu cara untuk mendapatkan kembali informasi yang telah dienkripsi.Kadang melalui proses berulang kali, (salah satu cara dengan Brute Force Attack yaitu serangan yang mencoba semua kemungkinan rangkaian kunci password) oleh peretas enkripsi. Kunci simetris artinya hanya satu kunci untuk mengunci (enkripsi) dan membuka (dekripsi). Asimetris jika ada dua kunci, kunci privat yang harus selalu disimpan/rahasia dan kunci publik/umum yang diumumkan di website misalnya dan digunakan oleh mitra transaksi anda untuk membuka (dekripsi) transaksi atau berita.

Tip mengapa email atau data transaksi perbankan harus dienkripsi jika ingin aman? Upayakan agar email text atau transaksi itu dijaga:

1. Kerahasiannya (Confidential) terhadap upaya penyadapan;
2. Integritasnya (integrity) agar data tidak diubah, dihapus, diganti;
3. Otentikasi (Authentication) dari data agar pengirim ter verifikasi, tidak anonim dan jelas. Certificate Authority (CA) adalah pihak ketiga yang membuat, memverifikasi publik & private key (kunci privat) untuk menjaga otentikasi pemiliknya.

Tangkis Konten Negatif dan Kecanduan

Konten-konten negatif seperti pornografi banyak berseliweran di Internet dan membahayakan pertumbuhan dan pikiran. Meskipun pemerintah sudah melakukan penyensoran satu situs, namun tumbuh 1000 situs baru, karena sifat Internet yang tanpa batas dan industri pornografi

yang booming. Berikut tipnya bagi Orang Tua dan Guru:

1. Mengedukasi agar anak-anak dan remaja menjauhi konten pornografi (namun juga pornoaksi, SARA, narkoba, dunia hitam dark web/deep web). Memberikan rasa tanggung jawab dan kepercayaan agar melakukan halhal yang positif seperti kursus dan kegiatan ekstra kurikuler sekolah, sehingga mereka tidak kecanduan menggunakan konten Internet dan Sosmed.
2. Mendidik anak-anak agar mengetahui bahwa Indonesia adalah negara hukum, yang memiliki hukum dan sangsi terkait pornografi, yang diatur dalam UU Pornografi No 44/2008 dan UU ITE No 11/ 2008. Penyebarluasan muatan yang melanggar kesusilaan, pornografi melalui Internet diatur dalam pasal 27 ayat 1 UU ITE mengenai Perbuatan yang dilarang dan dikenakan pidana penjara hingga enam tahun dan/atau denda hingga Rp 1 milyar.
3. Menemani anak-anak ketika sedang mengakses Internet atau letakan laptop atau perangkat lainnya di tempat yang terjangkau dari pengawasan orang tua.
4. Menggunakan alat pengontrol internet yang aman di gawai dan memonitor apa saja yang si-kecil lakukan di gawainya seperti apa yang ditonton atau games yang dimainkan memanfaatkan fitur Parental Control.
5. Memberi batas waktu bermain Internet kepada anak-anak, untuk mencegah anakanak kecanduan bermain Internet.

Menghindari & menangkal spaM, Malware, ransoMware, virus & spyware :

1. Rajin Update Sistem

   Malware/virus selalu mencari kelemahan (vulnerability) di setiap sistem agar bisa dibobol. Sistem operasi, software anti virus komputer dan smartphone harus diperbarui (update) sesuai rekomendasi pabrik, sehingga sistem keamanan sudah menggunakan sistem yang terbaru dan sudah diuji coba terhadap malware versi

sebelumnya

2. Gunakan & Update Anti Virus (AV)/ Anti Spam atau Anti Spyware/Worm untuk PC, Gawai dan Smartphone, agar selalu mempunyai penangkal virus/spam terbaru. Scan secara menyeluruh dan berkala untuk mencegah program malware, virus, spam, worm yang ingin masuk ke dalam komputer/smartphone anda
3. Backup dokumen, foto atau berkas penting lainnya ke flashdisk, harddisk cadangan (offline) atau ke layanan google dropbox (online). Agar memiliki data cadangan. Jika data anda hilang karena virus atau di sandera oleh ransomware yang meminta uang tebusan, maka dapat dipulihkan (recovery) dengan data backup
4. Jangan klik link web atau download file yang tidak dikenal. Karena dapat membangunkan malaware, virus, ransomware yang ada di file yang didownload atau attachment yang diklik, konsekwensinya data dalam gawai anda sudah terkontaminasi, termasuk daftar alamat (address book) digunakan oleh peretas untuk fase duplikasi malware dan penyebaran berikutnya
5. Berhati-hati gunakan wfi public. Terutama jika anda ingin melalukan transaksi keuangan, perbankan, ecommerce, credit cards serta aplikasi yang kritis dan strategis
6. Tidak gunakan perangkat pribadi di tempat bekerja, untuk memproses pekerjaan perusahaan

Cara penjagaan berlapis serangan cracker dari Internet dan dalam Sistem:

1. Memasang proteksi perimeter di peripheri (pagar) seperti Firewall, Router untuk sistem LAN internal perusahaan anda. Proxy di peripheri untuk memisahkan IP Internet Siber yang beresiko (compromised) dengan IP Private untuk semua PC dan gadget dilingkungan LAN Perusahaan. Proxy untuk memisahkan IP dunia cyber yang berbahaya (compromised) dengan IP Private untuk semua PC dan gadget

dilingkungan LAN Perusahaan.

2. Anti virus, Anti Spam, Anti Malware, Sensor konten di Server dan disetiap PC serta peralatan Anti Insider Threat yang merupakan pertahanan berlapis (defence in depth) bagi sebuah korporasi dan enterprise

Bahaya dan cara hindari Penipuan Phishing & social engineering di internet

Sosial Engineering (SosEng) menggunakan metode penyamaran, misalnya menyaru sebagai bos perusahaan dan menelpon satpam atau admin web untuk mendapatkan informasi rahasia seperti password. Modus SosEng yang lain adalah mengaku customer service sebuah bank atau kartu kredit dan minta informasi pribadi seperti pin atau data pribadi lainnya.

Phishing adalah upaya menyaru sebuah situs untuk melakukan penipuan. Kasus phishing terkenal pernah menimpa Klikbca.com Si cracker ini menyaru Klikbca.com dengan membuat beberapa situs yang mirip misalnya clickbca.com, clikbca.com atau Klik-bca.com. Nah korban yang tidak teliti membaca domain akan tertipu masuk situs phishing milik cracker. Selanjutnya cracker ini akan melakukan data mining pasword, login yang diketik oleh si korban, karena si korban sekarang bukan masuk ke situs BCA resmi tapi masuk ke situs si Cracker. Akhirnya si Cracker memiliki login dan password si korban dan dengan cepat menguras saldo si korban dengan cara phishing

1. Jangan panik dan tetap tenang menghadapi serangan phishing.
2. Segera hubungi call center atau datangi kantor dari perusahaan yang asli atau sebenarnya. Jelaskan anda ditenggarai menjadi korban phishing, agar informasi rahasia korban yang sudah dimiliki pelaku phishing segera di reset dan diubah agar pelaku phishing tidak dapat menguras rekening bank si korban.
3. Laporkan ke polisi agar situs penyamar pelaku phishing segera di blokir, ditutup dan pelaku phishing dikejar.
4. Rubah semua password dan login informasi agar tidak disusupi oleh cracker tersebut.

E. Bisnis di Bidang Teknologi Informasi

Beberapa alasan yang membuat bisnis perlu dilandasi oleh suatu etika :

a. Selain mempertaruhkan barang dan uang untuk tujuan keuntungan, bisnis juga mempertaruhkan nama, harga diri bahkan nasib umat manusia yang terlibat didalamnya.
b. Bisnis adalah bagian penting dari masyarakat, sebagai hubungan antar manusia bisnis membutuhkan etika yang mampu memberi pedoman bagi pihak yang melakukannaya.
c. Bisnis adalah kegiatan yang mengutamakan rasa saling percaya. Etika dibutuhkan untuk menumbuhkan dan memperkuat rasa saling percaya.

Sony keraf (1991) dalam buku Etika Bisnis : Membangun Citra Bisnis sebagai Profesi Luhur, memcatat beberapa hal yang menjadi prinsip dari etika bisnis, antara lain :

a. Prinsip otonomi
b. Prinsip kejujuran
c. Prinsip berbuat baik dan tidak berbuat jahat
d. Prinsip keadilan
e. Prinsip hormat pada diri sendiri

Beberapa kategori bisnis dibidang TI :

a. Bisnis dibidang Industri Perangkat Keras

   Bergerak dibidang rekayasa perangkat keras, contoh IBM, Compaq, dll.
b. Bisnis dibidang Rekayasa Perangkat Lunak

   Dilakukan oleh perusahaan yang menguasai teknik rekayasa, yaitu kegiatan engineering yang meliputi analisis, desain, spesifikasi, implementasi dan validasi

untuk menghasilkan produk perangkat lunak. Contoh : Microsoft, Adobe, dll.

c. Bisnis dibidang Distribusi dan Penjualan Barang

   Bisnis yang bergerak dibidang pemasaran produk komputer baik vendor ataupun secara pribadi.

d. Bisnis dibidang Pendidikan Teknologi Informasi

   Bisa berupa lembaga-lembaga kursus komputer sampai dengan perguruan tinggi bidang komputer. Contoh : BSI

e. Bisnis dibidang Pemeliharaan Teknologi Informasi

   Pemeliharaan bisa dilakukan oleh pengembang melalui divisi technical support atau spelialisasi bidang maintenance dan teknisi.

Tantanga umum bisnis di bidang TI :

a. Tantangan inovasi dan perubahan yang cepat
b. Tantangan pasar dan pemasaran di era globalisasi
c. Tantangan pergaulan internasional
d. Tantangan pengembangan sikap dan tanggung jawab pribadi
e. Tantangan pengembangan sumber daya manusia