**CYBER ETHICS DAN KEJAHATAN KOMPUTER**

1. **Cyber Ethics**

Etika adalah ilmu tentang apa yang baik dan apa yang buruk serta tentang hak dan kewajiban(akhlak). Etika apapun bentuknya adalah satu kesepakatan yang menunjukkan bahwa manusia adalah makhluk yang berbudaya dalam bersosialisasi. Manusia ingin dihargai sebagaimana ia berusaha menghargai orang lain. Etika bukan saja harus di pelajari pada kenyataan atau dunia nyata, melainkan pada dunia maya atau internet, etika pun harus ada dan perlu diterapkan.

Etika dalam berinternet biasa disebut dengan cyber ethics (etika cyber). Cyber ethics adalah suatu aturan tak tertulis yang dikenal di dunia IT. Suatu nilai-nilai yang disepakati bersama untuk dipatuhi dalam interaksi antar pengguna teknologi khususnya teknologi informasi. Tidak adanya batas yang jelas secara fisik serta luasnya penggunaan IT di berbagai bidang membuat setiap orang yang menggunakan teknologi informasi diharapkan bisa mematuhi cyber ethics yang ada. Cyber ethics memunculkan peluang baru dalam bidang pendidikan, bisnis, layanan pemerintahan dengan adanya kehadiran internet. Sehingga memunculkan netiket/nettiquette yaitu salah satu etika acuan dalam berkomunikasi menggunakan internet, berpedoman pada IETF (the internet engineering task force), yang menetapkan RFC (netiquette guidelies dalam request for comments).

Etika kehidupan berbangsa atau bernegara yang semula mudah sekali disosialisasikan karena orang berinteraksi secara langsung secara fisik, maka dalam dunia cyber upaya mensosialisasikan cyber ethics menjadi sulit sekali dilakukan karena jangkauan teritorinya sudah jauh lebh luas.

Sebenarnya cyber ethics dapat ditelaah dan dimengerti oleh pengguna internet, jika disadari terdapat etika kehidupan normal yang berlaku. Manusia tentu tidak ingin dirugikan dalam kehidupannya. Di dunia maya hal itu pun mungkin terjadi dan saat itulah terjadi pelanggaran cyber ethics, misalnya seseorang mengirimi email yang berisi informasi-informasi penjualan suatu produk dan karena email tersebut khawatir ditolak maka subyek email diubah menjadi sepenggal kalimat menarik yang tidak ada hubungan dengan isi email. Kontan saja si penerima merasa dirugikan, karena untuk membuka email ia memerlukan biaya koneksi ke internet, tidak seperti saat ia menerima surat pos biasa, ia tidak dikenakan biaya apapun. Kesalahan si pengirim adalah mengelabui email dengan subyek yang tidak tepat dan itulah salah satu pelanggaran etika dalam dunia cyber.

Seperti halnya etika dalam kehidupan bermasyarakat, sanksi yang diperoleh terhadap suatu pelanggaran adalah sanksi social. Sanksi social bisa saja berupa teguran atau bahkan dikucilkan dari kehidupan bermasyarakat. Demikian juga dengan pelanggaran etika berinternet. Sanksi yang akan diterima jika melanggar etika atau norma-norma yang berlaku adalah dikucilkan dari kehidupan berkomunikasi berinternet.

Cyber ethics berbeda dari *cyber law* yang memiliki pengertian seperangkat aturan hukum tertulis yang berlaku di dunia maya. Cyber law ini dibuat oleh negara untuk menjamin warga negaranya, karena dianggap aktivitas di dunia maya ini telah merugikan dan telah menyentuh kehidupan yang sebenarnya.

Beberapa cyber ethics yang sering dijumpai:

1. Etika menulis blog dan membuat website

Etika menulis di internet adalah suatu ke sopanan menulis yang meliputi ketentuan-ketentuan tertentu yang mengharuskan si penulis memenuhi syarat-syarat tertentu dalam menulis di internet. Kita tidak bisa semaunya dalam melakukan penulisan, jika kita masih mencari sumber tulisan kita melalui media internet. Tentunya kita wajib mencantumkan sumber dari mana kita dapatkan teori untuk tulisan yang kita buat. Untuk menghindari hal-hal yang di katakan plagiarisme dalam suatu hasil karya tulisan ataupun karya-karya yang lainnya.

Tata cara untuk menulis di dunia maya, meliputi banyak hal yang harus diperhitungkan agar etika dalam menulis yang dimaksud dapat terpenuhi. Adapun tata cara tersebut meliputi :

1. Mencantumkan sumber dari mana kita dapatkan teori yang menunjang pada tulisan yang dibuat meminta izin
2. Menulis tulisan dengan bahasa Indonesia yang baik dan benar
3. Tidak memposting tulisan atau hal-hal yang bersifat pornografi, menghina, mencemarkan nama baik, dan sebagainya.
4. Etika berkomunikasi menggunakan internet yang disebut netiket

Netiket : Contoh Etika Berinternet

Netiket atau *Nettiquette,* adalah etika dalam berkomunikasi menggunakan internet.

* Netiket pada *one to one communications*

Yang dimaksud dengan *one to one communications* adalah kondisi dimana komunikasi terjadi antar individu “face to face” dalam sebuah dialog.

* Netiket pada *one to many communications*

Konsep komunikasi  *one to meny communications* adalah bahwa satu orang bisa berkomunikasi kepada beberapa orang sekaligus. Hal itu seperti yang terjadi pada *mailing list* dan *net news.*

* Information services

Pada perkembangan internet, diberikan fasilitas dan berbagai layanan baru yang disebut layanan informasi *(information service).* Berbagai jenis layanan ini antara lain seperti *Gropher, Wais, Word Wide Web (WWW), Multi-User Dimensions (MUDs), Multi-User Dimensions which are object Oriented (MOOs)*

1. **Pentingnya Etika di Dunia Maya**

Beberapa alasan mengenai pentingnya etika dalam dunia maya adalah sebagai berikut:

1. Bahwa pengguna internet berasal dari berbagai negara yang mungkin memiliki budaya, bahasa dan adat istiadat yang berbeda-beda.
2. Pengguna internet merupakan orang-orang yang hidup dalam dunia *anonymouse,* yang tidak mengharuskan pernyataan identitas asli dalam berinteraksi.
3. Berbagai macam fasilitas yang diberikan dalam internet memungkinkan seseorang untuk bertindak etis seperti misalnya ada juga penghuni yang suka iseng dengan melakukan hal-hal yang tidak seharusnya dilakukan.
4. Harus diperhatikan bahwa pengguna internet akan selalu bertambah setiap saat dan memungkinkan masuknya “penghuni” baru didunia maya tersebut.
5. **Kejahatan Komputer**

Kejahatan komputer (**Cyber Crime)** adalah perbuatan melawan hukum yang dilakukan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis utama komputer dan jaringan telekomunikasi.

Banyak metode yang digunakan untuk melakukan kejahatan komputer. Metode-metode itu antara lain penipuan data, trojan horse, teknik salami, logic bomb dan kebocoran data. Penipuan data merupakan metode yang paling sederhana, aman dan lazim digunakan. Metode ini menyangkut pengubahan data sebelum atau selama proses pemasukan ke komputer.

1. **Faktor- faktor penyebab kejahatan komputer**

Beberapa faktor yang menyebabkan kejahatan komputer makin marak dilakukan antara lain adalah:

1. Akses internet yang tidak terbatas.
2. Kelalaian pengguna komputer. Hal ini merupakan salah satu penyebab utama kejahatan komputer.
3. Mudah dilakukan dengan resiko keamanan yang kecil dan tidak diperlukan peralatan yang super modern. Walaupun kejahatan komputer mudah untuk dilakukan tetapi akan sangat sulit untuk melacaknya, sehingga ini mendorong para pelaku kejahatan untuk terus melakukan hal ini.
4. Para pelaku merupakan orang yang pada umumnya cerdas, mempunyai rasa ingin tahu yang besar, dan fanatik akan teknologi komputer. Pengetahuan pelaku kejahatan komputer tentang cara kerja sebuah komputer jauh diatas operator komputer.
5. Sistem keamanan jaringan yang lemah. Sistem keamanan yang lemah, membuka peluang besar untuk pelaku kejahatan komputer.
6. Kurangnya perhatian masyarakat. Masyarakat dan penegak hukum saat ini masih memberi perhatian yang sangat besar terhadap kejahatan konvesional. Pada kenyataannya para pelaku kejahatan komputer masih terus melakukan aksi kejahatannya.
7. Belum adanya undang-undang atau hukum yang mengatur tentang kejahatan komputer.
8. **Jenis - Jenis Kejahatan Komputer**
9. **Berdasarkan jenis aktifitas yang dilakukannya**

Berdasarkan jenis aktifitas yang dilakukannya, kejahatan komputer dapat digolongkan menjadi beberapa jenis sebagai berikut:

* Unauthorized Access

Merupakan kejahatan yang terjadi ketika seseorang memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. *Probing* dan *port* merupakan contoh kejahatan ini.

* Illegal Contents

Merupakan kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau menggangu ketertiban umum, contohnya adalah penyebaran pornografi.

* Penyebaran virus secara sengaja

Penyebaran virus pada umumnya dilakukan dengan menggunakan email. Sering kali orang yang sistem emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.

* Data Forgery

Kejahatan jenis ini dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web database.

* Cyber Espionage, Sabotage, and Extortion

Cyber Espionage merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. Sabotage and Extortion merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

* Cyberstalking

Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail dan dilakukan berulang-ulang. Kejahatan tersebut menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya.

* Carding

Carding merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.

* Hacking dan Cracker

Istilah *hacker* biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut *cracker*. Boleh dibilang cracker ini sebenarnya adalah hacker yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas cracking di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai DoS (Denial Of Service). Dos attack merupakan serangan yang bertujuan melumpuhkan target (hang, crash) sehingga tidak dapat memberikan layanan.

* Cybersquatting and Typosquatting

Cybersquatting merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun typosquatting adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain. Nama tersebut merupakan nama domain saingan perusahaan.

* Hijacking

Hijacking merupakan kejahatan melakukan pembajakan hasil karya orang lain. Yang paling sering terjadi adalah Software Piracy (pembajakan perangkat lunak).

* Cyber Terorism

Suatu tindakan cybercrime termasuk cyber terorism jika mengancam pemerintah atau warga negara, termasuk cracking ke situs pemerintah atau militer.

1. **Berdasarkan motif kegiatan yang dilakukannya**

Berdasarkan motif kegiatan yang dilakukannya, cybercrime dapat digolongkan menjadi dua jenis sebagai berikut :

* Cybercrime sebagai tindakan murni kriminal

Kejahatan yang murni merupakan tindak kriminal merupakan kejahatan yang dilakukan karena motif kriminalitas. Kejahatan jenis ini biasanya menggunakan internet hanya sebagai sarana kejahatan. Contoh kejahatan semacam ini adalah Carding, yaitu pencurian nomor kartu kredit milik orang lain untuk digunakan dalam transaksi perdagangan di internet. Juga pemanfaatan media internet (webserver, mailing list) untuk menyebarkan material bajakan. Pengirim e-mail anonim yang berisi promosi (spamming) juga dapat dimasukkan dalam contoh kejahatan yang menggunakan internet sebagai sarana. Di beberapa negara maju, pelaku spamming dapat dituntut dengan tuduhan pelanggaran privasi.

* Cybercrime sebagai kejahatan ”abu-abu”

Pada jenis kejahatan di internet yang masuk dalam wilayah ”abu-abu”, cukup sulit menentukan apakah itu merupakan tindak kriminal atau bukan mengingat motif kegiatannya terkadang bukan untuk kejahatan. Salah satu contohnya adalah probing atau portscanning. Ini adalah sebutan untuk semacam tindakan pengintaian terhadap sistem milik orang lain dengan mengumpulkan informasi sebanyak-banyaknya dari sistem yang diintai, termasuk sistem operasi yang digunakan, port-port yang ada, baik yang terbuka maupun tertutup, dan sebagainya.

1. **Berdasarkan sasaran kejahatan**

Berdasarkan sasaran kejahatan, cybercrime dapat dikelompokkan menjadi beberapa kategori seperti berikut ini :

* Cybercrime yang menyerang individu (Against Person)

Jenis kejahatan ini, sasaran serangannya ditujukan kepada perorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut. Beberapa contoh kejahatan ini antara lain :

* Pornografi

Kegiatan yang dilakukan dengan membuat, memasang, mendistribusikan, dan menyebarkan material yang berbau pornografi, cabul, serta mengekspos hal-hal yang tidak pantas.

* Cyberstalking

Kegiatan yang dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya dengan menggunakan e-mail yang dilakukan secara berulang-ulang seperti halnya teror di dunia cyber. Gangguan tersebut bisa saja berbau seksual, religius, dan lain sebagainya.

* Cyber-Tresspass

Kegiatan yang dilakukan melanggar area privasi orang lain seperti misalnya Web Hacking. Breaking ke PC, Probing, Port Scanning dan lain sebagainya.

* Cybercrime menyerang hak milik (Againts Property)

Cybercrime yang dilakukan untuk menggangu atau menyerang hak milik orang lain. Beberapa contoh kejahatan jenis ini misalnya pengaksesan komputer secara tidak sah melalui dunia cyber, pemilikan informasi elektronik secara tidak sah/pencurian informasi, carding, cybersquating, hijacking, data forgery dan segala kegiatan yang bersifat merugikan hak milik orang lain.

* Cybercrime menyerang pemerintah (Againts Government)

Cybercrime Againts Government dilakukan dengan tujuan khusus penyerangan terhadap pemerintah. Kegiatan tersebut misalnya *cyber terorism* sebagai tindakan yang mengancam pemerintah termasuk juga cracking ke situs resmi pemerintah atau situs militer.

1. **Contoh Kasus Cyber Crime di Indonesia**

Beberapa contoh kasus cyber crime di Indonesia:

* Pencurian dan penggunaan account Internet milik orang lain.

Salah satu kesulitan dari sebuah ISP (Internet Service Provider) adalah adanya  
account pelanggan mereka yang “dicuri” dan digunakan secara tidak sah. Berbeda  
dengan pencurian yang dilakukan secara fisik, “pencurian” account cukup  
menangkap “user id” dan “password” saja. Hanya informasi yang dicuri.  
Sementara itu orang yang kecurian tidak merasakan hilangnya “benda” yang  
dicuri. Pencurian baru terasa efeknya jika informasi ini digunakan oleh yang tidak  
berhak. Akibat dari pencurian ini, penggunan dibebani biaya penggunaan account  
tersebut. Kasus ini banyak terjadi di ISP.

* Membajak situs web.

Salah satu kegiatan yang sering dilakukan oleh cracker adalah mengubah halaman  
web, yang dikenal dengan istilah deface. Pembajakan dapat dilakukan dengan  
mengeksploitasi lubang keamanan.

* Denial of Service (DoS) dan Distributed DoS (DDos) attack.

DoS attack merupakan serangan yang bertujuan untuk melumpuhkan target (hang,  
crash) sehingga dia tidak dapat memberikan layanan. Serangan ini tidak  
melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi dengan  
hilangnya layanan maka target tidak dapat memberikan servis sehingga ada  
kerugian finansial. Bagaimana status dari DoS attack ini? Bayangkan bila  
seseorang dapat membuat ATM bank menjadi tidak berfungsi. Akibatnya nasabah bank tidak dapat melakukan transaksi dan bank (serta nasabah) dapat mengalami kerugian finansial. DoS attack dapat ditujukan kepada server (komputer) dan juga dapat ditargetkan kepada jaringan (menghabiskan bandwidth). Tools untuk melakukan hal ini banyak tersebar di Internet. DDoS attack meningkatkan serangan ini dengan melakukannya dari berberapa (puluhan, ratusan, dan bahkan ribuan) komputer secara serentak. Efek yang dihasilkan lebih dahsyat dari DoS attack saja.

* Kejahatan yang berhubungan dengan nama domain.

Nama domain (domain name) digunakan untuk mengidentifikasi perusahaan dan  
merek dagang. Namun banyak orang yang mencoba menarik keuntungan dengan  
mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha  
menjualnya dengan harga yang lebih mahal. Pekerjaan ini mirip dengan calo  
karcis. Istilah yang sering digunakan adalah cybersquatting. Masalah lain adalah  
menggunakan nama domain saingan perusahaan untuk merugikan perusahaan  
lain. (Kasus: mustika-ratu.com) Kejahatan lain yang berhubungan dengan nama  
domain adalah membuat “domain plesetan”, yaitu domain yang mirip dengan  
nama domain orang lain. (Seperti kasus klikbca.com) Istilah yang digunakan saat  
ini adalah typosquatting.

1. **Penanggulangan dan Solusi Cyber Crime**

Aktivitas pokok dari cybercrime adalah penyerangan terhadap content, computer system dan communication system milik orang lain atau umum di dalam cyberspace. Fenomena cybercrime memang harus diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya. Cybercrime dapat dilakukan tanpa mengenal batas teritorial dan tidak memerlukan interaksi langsung antara pelaku dengan korban kejahatan. Berikut ini cara penanggulangannya :

1. **Mengamankan sistem**

Tujuan yang nyata dari sebuah sistem keamanan adalah mencegah adanya perusakan bagian dalam sistem karena dimasuki oleh pemakai yang tidak diinginkan. Pengamanan sistem secara terintegrasi sangat diperlukan untuk meminimalisasikan kemungkinan perusakan tersebut. Membangun sebuah keamanan sistem harus merupakan langkah-langkah yang terintegrasi pada keseluruhan subsistemnya, dengan tujuan dapat mempersempit atau bahkan menutup adanya celah-celah unauthorized actions yang merugikan. Pengamanan secara personal dapat dilakukan mulai dari tahap instalasi sistem sampai akhirnya menuju ke tahap pengamanan fisik dan pengamanan data. Pengaman akan adanya penyerangan sistem melaui jaringan juga dapat dilakukan dengan melakukan pengamanan FTP, SMTP, Telnet dan pengamanan Web Server.

1. **Penanggulangan Global**

The Organization for Economic Cooperation and Development (OECD) telah membuat guidelines bagi para pembuat kebijakan yang berhubungan dengan computer-related crime, dimana pada tahun 1986 OECD telah memublikasikan laporannya yang berjudul Computer-Related Crime : Analysis of Legal Policy. Menurut OECD, beberapa langkah penting yang harus dilakukan setiap negara dalam penanggulangan cybercrime adalah :

* Melakukan modernisasi hukum pidana nasional beserta hukum acaranya.
* Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.
* Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan cybercrime.
* Meningkatkan kesadaran warga negara mengenai masalah cybercrime serta pentingnya mencegah kejahatan tersebut terjadi.
* Meningkatkan kerjasama antarnegara, baik bilateral, regional maupun multilateral, dalam upaya penanganan cybercrime.

**DAFTAR PUSTAKA**

* <http://ranggablack89.wordpress.com/2012/04/01/cyber-crime-definisi-jenis-jenis-dan-cara-penanggulangannya/>
* h ttp://rizkasm.blogspot.com/2013/04/cyber-ethics\_1.html