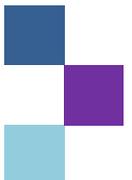


Berbagai Isu dan Best-Practices dalam Bekerja di Dunia Teknologi Informasi

Dari buku “**Digital Planet: Tomorrow’s Technology and You**” oleh George Beekman & Ben Beekman, 10th edition, Pearson, 2012 dan lecture notes oleh Inggriani Liem: “**Pemanfaatan IT, Komputer, E-mail, dan Internet**”



KU1072/Pengenalan Teknologi Informasi B
Tahap Tahun Pertama Bersama
Institut Teknologi Bandung





Tujuan

- Mahasiswa memahami beberapa isu di seputar perkembangan Teknologi Informasi
- Mahasiswa mengetahui beberapa *best practices* pemakaian komputer, e-mail, dan Internet
- Mahasiswa memahami beberapa etika dalam bekerja di dunia Teknologi Informasi



Dunia TI, Dunia Maya

- Kemajuan teknologi, terutama di bidang Teknologi Informasi (TI) membawa perubahan kehidupan.
- Komputer sudah merupakan bagian dari *tools* yang digunakan dalam pekerjaan profesi apa pun, dan PC (termasuk *laptop*) bahkan sudah bukan hanya alat kantor, tapi sekaligus alat *entertainment*
- Dunia Internet, dunia maya: dunia *baru* yang memungkinkan siapapun dapat memasukinya, tanpa tergantung ruang dan waktu. Adalah manusia yang masuk ke dunia maya itu.



Dunia TI sebagai Sumber Belajar Seumur Hidup

- Dunia TI sekarang menjadi sumber belajar yang tak ada habisnya. Bahan-bahan belajar tersedia dan dapat diakses dengan mudah.
- Referensi (ensiklopedia, kamus, atlas, referensi medis, dll.) tersedia dalam bentuk digital melalui Internet, aplikasi *smartphone*, CD/DVD
- Internet menyediakan blog, forum, website, dan berbagai pilihan media untuk belajar apa saja di mana saja → memungkinkan *distant learning*
- *Edutainment* mengombinasikan pendidikan dengan hiburan



TI juga berpengaruh pada dunia kerja

- TI membawa efisiensi dalam berbagai pekerjaan manusia
- Beberapa ahli memprediksi automasi, melalui TI, akan membuka berbagai peluang kerja yang tidak terbatas
- Beberapa teknologi juga membuka “gembok” kreativitas manusia
- **Globalisasi:** menciptakan “world-wide workers” dan membuka pasar pada level global



BEBERAPA ISU DALAM DUNIA TI



Resiko Potensial Pemanfaatan TI

- Ancaman terhadap norma dan etika
- Ancaman terhadap privasi pribadi
- Ancaman “kecanduan” dan kekerasan di dunia maya
- Ancaman dari *high-tech crime*
- Kesulitan dalam mendefinisikan dan melindungi Hak atas Kekayaan Intelektual
- Ancaman automasi dan dehumanisasi pekerjaan terhadap meningkatnya jumlah pengangguran
- Penggunaan informasi dalam kepentingan politik



Norma, Etika dan Peraturan

- Norma dan etika: menyangkut moral, dan hanya “rambu-rambu”, hati nurani anda harus berperan.
- Peraturan, regulasi: lebih operasional, jelas ada statement, regulasi, hukuman, sanksi. Peraturan dibuat agar hidup bersama menjadi “nyaman”, bukan mempersulit.
- Jika melanggar norma/etika, seharusnya “malu”. Jika melanggar peraturan, akan dihukum supaya anggota komunitas tahu dan tidak melanggarnya.
- Carilah bahan-bahan di Internet menggunakan *search engine* dengan mengetikkan *keyword* “**netiquette**”, “**net-ethics**”.



Kebebasan vs tanggung jawab sosial

- Internet memberikan kebebasan untuk berbicara dan mengemukakan pendapat, sehingga juga dieksploitasi untuk tujuan-tujuan yang tidak bertanggung jawab
- Pemerintah menyediakan peraturan : **UU Informasi dan Transaksi Elektronik no. 11/2008**

Carilah di internet mengenai isi UU ini!

- Kita tetap bertanggung jawab atas apapun yang kita pikirkan/ucapkan/tuliskan secara online/offline
- Etika adalah prinsip/standar moral yang dapat digunakan sebagai petunjuk perilaku, tindakan, dan pilihan



Computer Ethics

- *Know the rules and the law.*
- *Don't assume that it's okay if it's legal.*
- *Think scenarios.*
- *When in doubt, talk it out.*
- *Make yourself proud.*
- *Remember the golden rule.*
- *Take the long view.*
- *Do your part.*



Ancaman terhadap Privasi (1)

- Meletakkan data pribadi secara online → tersimpan di *database* server
 - Dapat tersebar dengan sangat mudah di atas internet
 - Ketahuilah hak-hak Anda terhadap data
- Perusahaan-perusahaan *e-commerce* mungkin akan memanfaatkan data pribadi untuk berbagai keperluan (misalnya iklan)
- Dewasa ini privasi semakin berkurang
 - Di tempat kerja dapat dilakukan monitoring yang ketat terhadap pekerja dengan memanfaatkan TI
 - Penggunaan kamera surveilans di tempat-tempat umum



Ancaman terhadap Privasi (2)

- Teknologi informasi memungkinkan dilakukan penyadapan terhadap pribadi, organisasi, atau bahkan negara
 - Aparat hukum sering menggunakan penyadapan sebagai sarana untuk mendapatkan bukti kejahatan → ada undang-undang yang mengatur
 - Akhir-akhir ini sedang marak isu mengenai penyadapan antar negara



Your Privacy Rights

- ❑ Jangan mudah memberikan/menyebar nomor KTP, SIM, telepon, email, HP, nomor rekening, dan data-data penting lain, baik milik sendiri maupun orang lain
- ❑ Jangan mudah memberikan informasi pribadi
- ❑ Jangan mudah mengizinkan *sharing* informasi pribadi
- ❑ PIKIR sebelum POST!
- ❑ Gunakan teknologi untuk memproteksi hak pribadi
- ❑ Jika ada informasi yang merusak tentang diri Anda, perbaiki!



Ancaman “Kecanduan” dan “Kekerasan”

- Anak-anak zaman sekarang menghabiskan 25 jam atau lebih setiap minggu untuk digital media
 - Tidak terlibat dalam kegiatan fisik dan imajinatif yang dikembangkan sendiri
 - Lebih beresiko pada stres, depresi, dan isolasi sosial
 - Perubahan pada sikap dan cara otak bekerja
- Beberapa *online gamers* bisa menghabiskan 40-80 jam setiap minggu
- Kecanduan *game* adalah salah satu problem anak-anak zaman sekarang → termasuk problem anak ITB
- Riset membuktikan ada kaitan antara *game* bertema kekerasan dengan kekerasan di dunia nyata



Menghindari kecanduan & kekerasan

- Kurangi waktu di depan komputer
- Gunakan *filtering software* (khususnya bagi anak-anak)
- Perbanyak kegiatan fisik → main, olahraga, rekreasi
- Bergaul dengan teman fisik, bukan teman virtual, apalagi komputer
- Ikuti kegiatan-kegiatan sosial → unit kegiatan, himpunan, klub, dll.
- Jika ada masalah, bicarakan secara langsung → tidak curhat melalui *social media*
- Jaga hubungan baik dengan keluarga dan teman



Ancaman Cybercrime

- **Computer crime (kejahatan komputer)**: semua kejahatan yang dilakukan melalui pengetahuan dan penggunaan teknologi komputer
- Di seluruh dunia, bisnis dan pemerintah kehilangan milyaran dollar setiap tahun karena kejahatan komputer
- Kebanyakan kejahatan komputer dilakukan oleh orang dalam dan sering ditutupi karena malu



Cybercrime menurut UU ITE no. 11/2008

Beberapa materi perbuatan yang dilarang (*cybercrimes*) yang diatur dalam UU ITE, antara lain:

1. **konten ilegal**, yang terdiri dari, antara lain: kesusilaan, perjudian, penghinaan/pencemaran nama baik, pengancaman dan pemerasan (Pasal 27, Pasal 28, dan Pasal 29 UU ITE);
2. **akses ilegal** (Pasal 30);
3. **intersepsi ilegal** (Pasal 31);
4. **gangguan terhadap data** (data interference, Pasal 32 UU ITE);
5. **gangguan terhadap sistem** (system interference, Pasal 33 UU ITE);
6. **penyalahgunaan alat dan perangkat** (misuse of device, Pasal 34 UU ITE);



Pencurian terkait Teknologi Komputer (1)

- Adalah kejahatan komputer paling umum
- Pencurian fisik komputer: pencurian laptop, HP, smartphome, tablet, dll.
- **Pencurian identitas pribadi**: sudah menjadi industri kriminal yang cukup besar
 - Dipicu oleh ketidakhati-hatian saat *online* atau kesalahan penilaian
 - Butuh bertahun-tahun untuk membersihkan dampak dari pencurian identitas



Pencurian terkait Teknologi Komputer (2)

- Pencurian hak milik intelektual:
 - ***Social engineering***: menggunakan cara-cara penipuan untuk mendapatkan informasi yang bersifat sensitif dari orang lain
 - ***Spoofing***: berpura-pura menjadi orang lain dan melakukan tindakan-tindakan yang bersifat mengganggu/kriminal
 - ***Phishing***: mendapatkan informasi penting (username, password, informasi kartu kredit, uang), dengan berpura-pura menjadi suatu pihak yang terpercaya dalam komunikasi elektronik



Perangkat Lunak Sabotase

- ✓ **Malware:** *malicious software*
- ✓ **Viruses:** mereplikasi diri sendiri ke dalam program yang tidak terinfeksi
- ✓ **Worms:** bereproduksi sampai komputer berhenti bekerja
- ✓ **Trojan horses:** membawa program yang merusak
 - **Logic bomb** diprogram untuk bereaksi terhadap suatu event
 - **Time bombs** di-triger oleh event yang berbasis waktu
- ✓ **Spyware:** mengumpulkan informasi tanpa sepengetahuan user
- ✓ **Spybots:** mengomunikasikan data ke pihak lain melalui Internet



Hacking & Electronic Trespassing

- **Hackers:** orang yang memasuki sistem komputer orang lain tanpa izin
- **Cracking:** criminal hacking
- **Hactivists:** hacking sebagai salah satu bentuk aktivitas politik
- **Botnets:** jaringan komputer yang telah dibajak
- **DOS (denial of service):** serangan dengan cara membombardir server atau website sebegitu rupa sehingga menghentikan operasi server atau website tersebut



Beberapa Teknologi Keamanan Komputer

- ✓ ***Antivirus software:*** serum untuk virus, sekaligus mencari virus baru
- ✓ ***Security patches:*** mendeteksi potensi kebocoran keamanan
- ✓ ***Firewalls:*** menjaga akses tidak terotorisasi terhadap jaringan internal
- ✓ ***Encryption software:*** transmisi data dalam bentuk acak untuk mengamankannya dalam proses pengiriman
- ✓ ***Audit-control software:*** digunakan untuk memantau dan menyimpan transaksi komputer sehingga dapat diketahui jejak aktivitasnya



Beberapa Tips untuk Keamanan Komputer

- Back up data secara reguler dan simpan back up secara fisik di tempat yang berbeda dengan komputer
 - Back up dapat disimpan secara online
- Pasang antivirus dan update secara reguler
- Update sistem operasi secara reguler → beberapa fitur keamanan sering ditambahkan
- Pasang firewall
- Berinternet secara sehat
 - Jangan buka link, mail, pop-up, iklan, dll. yang tidak dipercaya
 - Tidak meletakkan informasi secara berlebihan



Protecting Yourself from Identity Theft

- *Make your online purchases using a credit card or PayPal.*
- *Scan your bills promptly.*
- *Get a separate credit card for online transactions.*
- *Make sure a secure Web site is managing your online transaction.*
- *Don't disclose personal information over the phone.*
- *Handle email with care.*
- *Don't put your Social Security number on your checks.*
- *Shred sensitive mail before you recycle it.*
- *Keep your wallet thin.*
- *Copy your cards.*
- *Report identify theft promptly.*

You think hacking is fun?? Think again!

Undang-Undang Informasi dan Transaksi Elektronik No. 11/2008

Pasal 30

(3) Setiap Orang dengan sengaja dan tanpa hak atau melawan **hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.**

Pasal 36

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang **mengakibatkan kerugian bagi Orang lain.**

Pasal 46

(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).

Pasal 51

(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 36 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

Be careful on what you post online!

Pasal 27

(3) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki **muatan penghinaan dan/atau pencemaran nama baik**.

Pasal 28

(1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan **berita bohong dan menyesatkan** yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

(2) Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk **menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA)**.

Pasal 45

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).



Pembajakan Perangkat Lunak dan HAKI

- **Pembajakan software**: duplikasi ilegal terhadap perangkat lunak yang memiliki hak cipta (copyright) → sangat sulit dikendalikan
- Banyak orang tidak tahu mengenai hukumnya, sebagian yang lain memilih tidak peduli
- Industri perangkat lunak kehilangan milyaran dollar setiap tahun dari pembajakan → yang terkena dampak khususnya adalah perusahaan kecil
- Perkiraan Business Software Alliance (BSA) : lebih dari sepertiga perangkat lunak yang beredar adalah bajakan

Crime Statistics > Software piracy rate (most recent) by country

DEFINITION: The piracy rate is the total number of units of pirated software deployed in 2007 divided by the total units of software installed.

Showing latest available data.

Rank	Countries	Amount
# 1	 Armenia:	93%
= 2	 Azerbaijan:	92%
= 2	 Moldova:	92%
= 2	 Bangladesh:	92%
# 5	 Zimbabwe:	91%
# 6	 Sri Lanka:	90%
# 7	 Yemen:	89%
# 8	 Libya:	88%
# 9	 Venezuela:	87%
= 10	 Iraq:	85%
= 10	 Vietnam:	85%
= 12	 Pakistan:	84%
= 12	 Indonesia:	84%
= 12	 Algeria:	84%
= 12	 Cameroon:	84%
# 16	 Ukraine:	83%
= 17	 China:	82%
= 17	 Paraguay:	82%

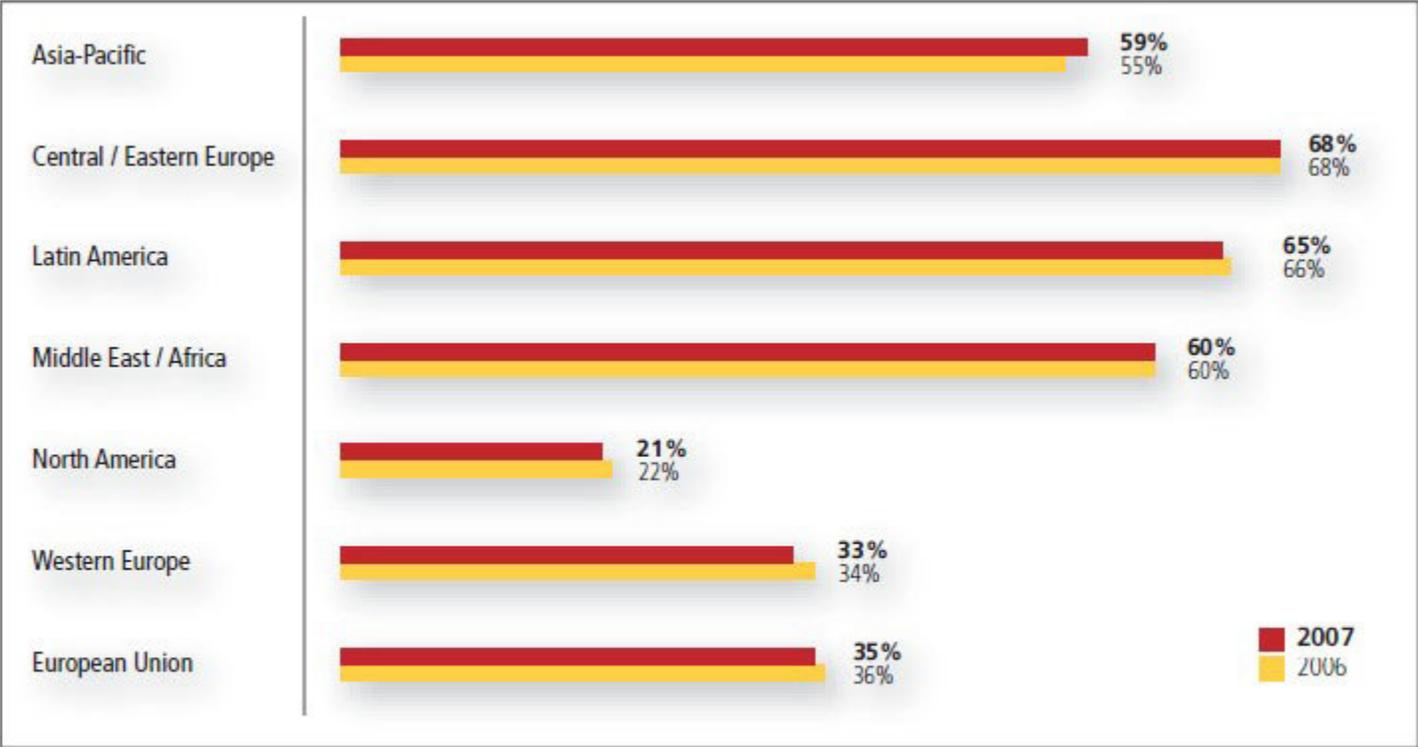
Sumber:

http://www.nationmaster.com/red/graph/crime-software-piracy-rate&b_printable=1

Akses: 2 Sept 2013



Figure 1. Piracy Rate by Region



Global Piracy Rates menurut Global Piracy Software Study: piracy rate berdasarkan region di dunia untuk tahun 2006 dan 2007

Sumber: http://www.tweakguides.com/Piracy_4.html

Akses : 2 Sept 2013





HAKI dan Hukum

- **HAKI (Hak atas Kekayaan Intelektual)** : hasil aktivitas intelektual dalam bidang seni, sains, dan industri
- **Hak cipta (copyright)** : melindungi buku, lagu, penampilan panggung, lukisan, foto, dan film
- **Trademark** : melindungi simbol, gambar, suara, warna, dan bau
- **Paten** : penemuan mekanik
- **Kontrak** : melindungi rahasia-rahasia perdagangan
- Menurut hukum, perangkat lunak tidak termasuk dalam kategori apa pun



Proprietary, Free, Open Source SW

	Freely Modifiable	Free Use
Proprietary SW	x	x
Free SW	x	✓
Open Source SW	✓	✓

Productivity on a Student Budget

- ✓ Software murah atau *free* tersedia sebagai alternatif:

Software	Alternatif untuk:
OpenOffice	Microsoft Office
Zoho Writer or Google Docs	Microsoft Word
Zoho Sheet or Google Spreadsheet	Microsoft Excel
Zoho Show or OpenOffice Impress	Microsoft PowerPoint
Scribus	Desktop Publishing

- ✓ Kebanyakan program dapat menyimpan file dalam format yang kompatibel dengan MS Office sehingga dapat bekerja dengan para user MS Office



Ancaman Automasi dan Globalisasi (1)

- Dewasa ini orang semakin terbiasa menggunakan dan bekerja dengan mesin (komputer)
- Kemungkinan besar, dalam waktu dekat, mesin akan dapat melakukan kebanyakan pekerjaan yang saat ini dilakukan oleh manusia
- Automasi menjadi isu besar, terutama bagi jutaan pekerja yang pekerjaannya terancam oleh mesin dan mereka yang tidak terampil dan tidak terdidik dengan TI
- Banyak ahli berpendapat bahwa automasi akan membawa pada jumlah pengangguran yang masif dan bencana ekonomi

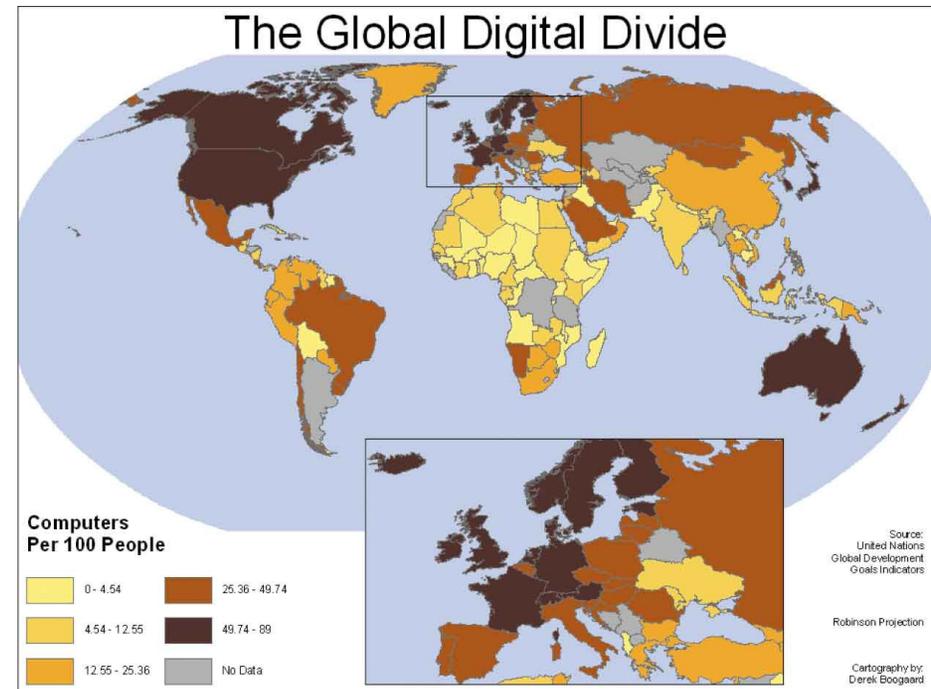


Ancaman Automasi dan Globalisasi (2)

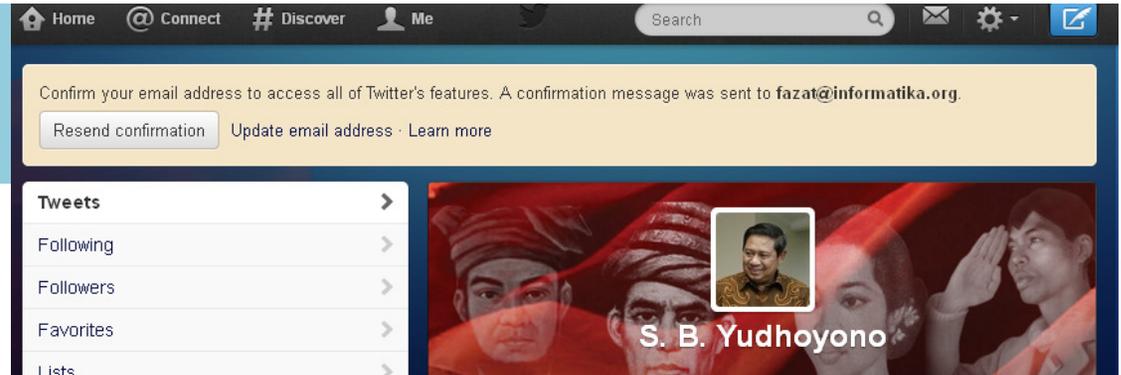
- Globalisasi:
 - Membawa para pekerja melintasi batas-batas negara → dapat menjadi ancaman bagi negara dengan sumber daya manusia yang tidak dapat bersaing
 - Membuka pasar dalam negeri ke masyarakat dunia → ancaman konsumerisme dan komersialisasi

Digital Divide

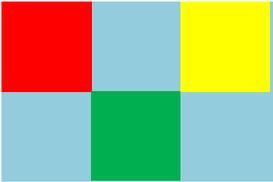
- *Digital divide* membagi dunia menjadi area-area dengan akses TI tinggi dengan akses TI yang rendah
- Negara-negara dengan akses TI yang rendah mempunyai potensi yang lebih rendah untuk bersaing → termasuk Indonesia



IT dalam Dunia Politik (1)



- Dunia politik memanfaatkan IT secara intensif untuk menyebarkan informasi dan membentuk opini masyarakat
- Social media, blog, forum, dan websites adalah media yang efektif untuk menyebarkan informasi dan berkampanye tentang isu tertentu
- Lembaga survey memanfaatkan berbagai teknologi untuk menjangkau pendapat masyarakat
- **Black campaign** sebagaimana **white campaign** bisa disebar dengan cepat melalui Internet dan media lain

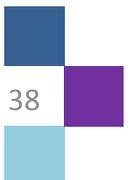


IT dalam Dunia Politik (2)

- Masyarakat terbebani oleh informasi yang berlebihan tentang politik → sulit/mustahil diketahui mana informasi yang benar/akurat, dan mana yang tidak
- Isu-isu yang meresahkan sering diedarkan oleh pihak-pihak yang tidak bertanggung jawab untuk menggoncangkan situasi negara → khususnya menjelang event besar, mis. Pemilu
- Beberapa tips:
 - Waspada dan bijak dalam menanggapi semua isu yang beredar. Pahami bahwa tidak semua isu selalu benar.
 - Tidak perlu ikut menyebarkan isu-isu yang tidak diketahui kebenarannya dan berpotensi meresahkan masyarakat.
 - Ikuti diskusi yang bermanfaat dan berdiskusilah secara sehat.
 - Laporkan kepada yang berwajib jika menerima isu yang berpotensi merusak ketentraman masyarakat.



BEBERAPA BEST PRACTICES DALAM PEMANFAATAN TI





PC (Personal Computer) (1)

- PC (termasuk *laptop*) bukan hanya sebagai alat bekerja, melainkan juga alat entertainment.
- Harus membedakan antara keduanya : PC sebagai “*work station*” atau PC sebagai sarana *entertainment*. Contoh: *games* adalah untuk *entertainment*
- Di kampus/lab/kantor [kelak], PC harus diperlakukan sebagai *work station dan* sepantasnya.



PC (Personal Computer) (2)

- Setting PC sesuai kantor, dengarkan musik dengan *headphone*.
- Penamaan dan pengaturan direktori sistematis, pisahkan *file* pribadi dengan kedinasan.
- Tidak menyimpan *file* yang kurang relevan dengan urusan “dinas” di PC kantor/lab.
- Melakukan *backup dan pembersihan* berkala, terutama *recycle bin*.
- Meninggalkan PC di kantor/lab dalam keadaan “benar”
- Pasang *username/password* pada PC (laptop) pribadi



User Id

- Pemberian *user id* adalah kepercayaan, anda harus menghormatinya.
- *User id* tidak dipakai “rame-rame”.
- *User id* diberikan sesuai “*role*”, *peran*
- Jangan bekerja dengan *user id* orang lain, beberapa sistem mencatat dengan diam-diam.
- Contoh: pemakaian *user id* A13, pemakaian *user id* di sistem akademik, di sistem laboratorium dan praktikum,

- *Password* terkait dengan *user id*, yang harus dijaga kerahasiaannya:
 - Tidak memberikan *password* ke orang lain.
 - Tidak minta *password* ke orang lain dan bekerja dengan *password* itu.
 - Tidak mencatat *password* dan membiarkan di tempat yang mudah diakses.
- *Password* harus secara rutin diganti
- *Password* tidak mudah ditebak:
 - Minimal 8 karakter.
 - Mengandung huruf besar/kecil/angka, bukan tgl.lahir/nama isteri,
 - Bukan kata yang mudah ditebak.



E-mail (1)

- Perhatikan bagian : ***header*** (*To, CC, BCC, Subject*), ***body, signature***
- Saran :
 - *Subject* harus diisi; 1 e-mail per subject.
 - *Signature* harus diperhatikan (maksimum 4 baris, identitas jelas). *Body* dipisahkan dari *signature* dengan "--" diikuti "return".
 - Pakailah bahasa yang baik dan sopan untuk email bersifat "dinas". E-mail bukan SMS.
 - Perhatikan "*thread*". Mulai rubrik baru dengan mengkomposisi e-mail baru



E-mail [2]

- *E-mail account* adalah pribadi, wajib dibuka pemiliknya.
- Tidak membuka e-mail orang lain (walaupun atasan/teman/saudara).
- Periksa baik-baik sebelum membuka email, adakah *spam* yang membawa virus. *Delete* sesegera mungkin e-mail yang tidak relevan.
- Pikir dan teliti sebelum *send*. Mungkin saja email anda akan di-forward ke siapapun.



Beberapa *E-mail Ethics* (1)

- Dalam dunia e-mail, teks yang diketik dengan huruf besar berarti TERIAKAN (*SHOUTING*) dan beberapa pembaca mengartikannya sangat kasar. Gunakan huruf besar hanya untuk menekankan hal penting.
- Penekanan dilakukan dengan **bold** atau *asteriks*
- *Mem-forward*: Tuliskan referensi sumbernya dan bagaimana memperoleh kopian-nya. Jangan melakukan *forward* ke *mailing list* tanpa seizin penulis asalnya



Beberapa *E-mail Ethics* (2)

- Tindakan tidak layak via e-mail (tapi tidak hanya terbatas kepada hal berikut):
 - Memposting sesuatu yang melanggar hukum dalam sebuah sistem
 - Pemakaian bahasa/pesan yang kasar baik untuk pesan pribadi maupun untuk umum,
 - Mengirimkan pesan yang memungkinkan kerusakan di tempat penerima
 - Pengiriman surat berantai atau menyebarkan surat pribadi
 - Tindakan-tindakan yang menyebabkan terganggunya jaringan komputer



Netiquette and Messaging Etiquette

- *Say what you mean; say it with care.*
- *Keep it short.*
- *Proofread your messages.*
- *Don't assume you are anonymous.*
- *Learn the “nonverbal” language of the Net.*
- *Know your abbreviations.*
- *Keep your cool.*
- *Don't be a source of spam.*
- *Say no—and say nothing—to spam.*



Milis sebagai Sarana Kerja (1)

- Memahami etika komunikasi dalam milis, menghormati “*thread*”.
- Menyimpan *notification*, cara mendaftar dan berhenti sebagai anggota. Sebagai peserta kelas, anda secara otomatis didaftarkan pada milis kelas.
- Memahami cara membuka *archive*, mengetahui siapa anggotanya.
- Ingat bahwa satu alamat mengandung banyak alamat anggotanya.



Milis sebagai Sarana Kerja (2)

- **Tidak disarankan:** berlangganan ke mailing list bervolume besar untuk topik yang bukan urusan kantor/akademik dengan alamat kantor/kampus.
- **Disarankan:** untuk memakai alamat di situs lain (misalnya gmail, yahoo) untuk menjadi anggota *mailing list* yang setiap hari membanjiri kotak surat anda dengan banyak sekali surat.



Software & Softcopy (1)

- *Software/softcopy* adalah buah pikiran dan buah kerja manusia yang selayaknya dihargai.
- *Software/softcopy* tidak kelihatan. Gampang dicopy, dicuri, disebarkan tanpa kita merasa kehilangan. Gampang terjadi kejahatan tanpa tampak mata. Contek-mencontek sangat gampang. Kita harus “kuat imannya”.
- Misalnya dalam praktikum/tugas, godaan untuk meng-*copy* pekerjaan teman sangat besar.
- Sangat berhati-hati dalam melakukan *copy/paste* dan tidak lupa menyebutkan sumbernya jika memakai bahan orang lain yang kita ambil dengan mudah dari Internet.



Software & Softcopy (2)

- Orang mengira pemakaian SW itu gampang! Analogi : menyopir. Pemakaian SW : aspek teknis, **aspek lain (sikap, kegunaan, efisiensi, konsep di baliknya,...)**
- Contoh : memakai MS Word ada sampai 7 tingkatan: mesin ketik, mesin ketik plus (*copy/paste,..*), *formatter*, pembantu kesalahan, *style*, *generate table of contents/reference*, *mail & merge*, memanfaatkan *object* dan *macro*.
- Pelajari penggunaan SW secara efektif untuk mendukung pekerjaan



Internet (1)

- Memakai Internet di kampus untuk keperluan belajar, mencari informasi/literatur. Tidak mengakses situs-situs yang kurang relevan dengan pelajaran.
- Tidak memakan *bandwidth* dengan melakukan *download file* berukuran besar.
- Menggunakan browser dengan baik. Tidak lupa melakukan *log out* [bukan hanya exit dari browser]



Internet (2)

- Memahami aturan pengalamatan dan “domain”.
- Harus selektif. Merupakan “godaan”, sebab bisa kemana-mana dan menghabiskan waktu.
- Pakailah Internet untuk pendukung pekerjaan.
- Tidak mem-*print*, menghabiskan tinta kantor untuk mem-*print* berita-berita Internet.



HW dan Jaringan

- Jaman sekarang hampir semua hardware terhubung jaringan
- Perhatikan bahwa sekali anda *login*, anda memasuki suatu komunitas tanpa batas
- Anda harus tahu diri, dan berkelakuan sesuai norma dan etika yang berlaku
- Berikan contoh pemakaian jaringan yang tidak seharusnya.



Jejaring Sosial (1)

- Facebook, Twitter, YM, ... to name a few
- Menghubungkan orang seluruh dunia → dunia tanpa batas ruang dan waktu.
- Harus disadari betul manfaat dan *mudharat*-nya!
- Dapat digunakan sebagai sarana komunikasi terkait pekerjaan, tetapi **hati-hati** dalam memilih informasi yang disebar. Jangan sampai menyebarkan informasi yang hanya boleh diketahui orang/kelompok tertentu kepada semua orang → manfaatkan *group*.



Jejaring Sosial (2)

- Hati-hati menulis status atau *tweet*! Pikir sebelum *send*! Tulisan Anda bisa memberikan dampak di seluruh belahan dunia.
- Tidak menyebarkan informasi, baik tulisan, gambar, video, dll., yang berbau SARA, pornografi, melanggar hukum, dan hal-hal lain yang mengganggu masyarakat. Sudah ada kasus mahasiswa ITB diskors karena menyebarkan informasi berbau SARA.
- Batasi informasi pribadi yang diletakkan di ruang publik.

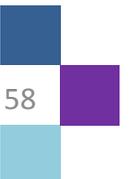


Pemakaian Fasilitas Bersama

- Contoh: *shared printer, shared file, shared directory*
- Perhatikan “jatah”, dan jangan membuat orang lain tidak bisa bekerja.



PENUTUP





Safe Computing

- Share with care.
- Beware of email bearing gifts.
- Handle shareware and freeware with care.
- Don't pirate software.
- Disinfect regularly.
- Take your passwords seriously.
- If it's important, back it up.
- If it's sensitive, lock it up.
- Treat your removable discs and drives as if they contained something important.
- If you're sending sensitive information, consider encryption.



Online Survival Tips

- *Let your system do as much work as possible.*
- *Store names and addresses in a computer-accessible address book.*
- *Don't share emails and passwords.*
- *Protect your privacy.*
- *Don't open suspicious attachments.*
- *Don't get hooked by a phishing expedition.*
- *Keep your security systems up to date.*
- *Cross-check online information sources.*
- *Beware of urban legends.*
- *Be aware and awake.*
- *Avoid information overload.*



Tantangan menjadi Pemakai di Lingkungan TI

- Materi di bidang TI berubah dengan cepat, sesuai dengan bidang itu sendiri.
- *Tools* berkembang cepat, versi *software* selalu berganti.
- Kita harus terus menerus belajar dan beradaptasi.
- Karena itu: hal yang prinsip dan konseptual perlu dikuasai.

History of the Future



- Teknologi hari ini memunculkan berbagai kemungkinan masa depan yang menggairahkan, tetapi juga bukannya tanpa masalah
- Pertumbuhan eksponensial dari kekuatan komputasi memungkinkan teknologi yang dulu tampak sangat jauh akan segera menjadi makanan sehari-hari
- Kita akan berhadapan banyak pertanyaan sulit yang terkait dengan legal (hukum), politik, sosial, ekonomi dan moral/etika