

Dunia Cyber dan dampak negatif (Cybercrime)

Iwan Setiawan, ST, MT

heroku.iih@gmail.com

- Istilah "cyber" diperkenalkan oleh William Gibson seorang penulis fiksi ilmiah (science fiction) dengan memperkenalkan istilah "cyberspace" dalam novelnya yang berjudul Neuromancer
- Perkembangan selanjutnya menjadi ruang elektronik (electronic space), yaitu sebuah masyarakat virtual yang terbentuk melalui komunikasi yang terjalin dalam sebuah jaringan komputer (interconnected computer networks).'

Iwan Setiawan, ST, MT

heroku.iih@gmail.com



Contoh

- Orang **Indonesia**, Melakukan transaksi melalui Internet dengan Perusahaan **Inggris**, dengan Lokasi server di **Amerika**
- Hukum mana yang digunakan?
- Kapan dan dimana transaksi terjadi?

Iwan Setiawan, ST, MT

heroku.iih@gmail.com

Informasi = Uang?

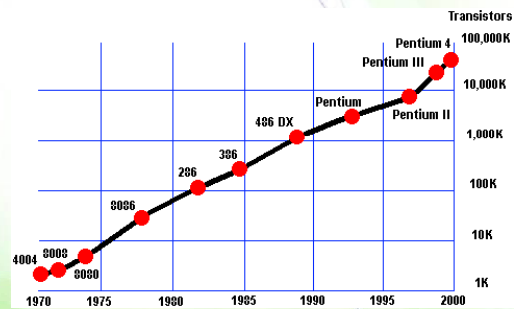
- ▶ Informasi memiliki nilai (value) yang dapat dijual belikan
 - Data-data nasabah, mahasiswa
 - Informasi mengenai perbankan, nilai tukar, saham
 - Soal ujian
 - Password, PIN
- ▶ Nilai dari informasi dapat berubah dengan waktu
 - Soal ujian yang sudah diujikan menjadi turun nilainya

Iwan Setiawan, ST, MT

heroku.iih@gmail.com

Technology Drivers

- Computer Technology
 - Moore's law: complexity doubles every 18 months
 - Good enough
- Storage Technology
 - Increases 3 times / year
 - Good enough
- Network Technology
 - Increase in speed, lower in price
 - But ... new bandwidth-hungry applications. The need for (more) speed!



Iwan Setiawan, ST, MT

heroku.ili@gnail.com

Perhatian terhadap keamanan informasi

- Mulai banyaknya masalah keamanan informasi
 - Virus, worm, trojan horse, spam
 - Hacking & cracking
 - Spyware, keylogger
 - Fraud (orang dalam), penipuan, pencurian kartu kredit
- Masalah security dianggap sebagai penghambat penerimaan penggunaan infrastruktur teknologi informasi

Iwan Setiawan, ST, MT

heroku.ili@gnail.com

Definisi Kejahatan Komputer

- Tavani (2000) memberikan definisi cybercrime, yaitu ***kejahatan dimana tindakan kriminal hanya bisa dilakukan dengan menggunakan teknologi cyber dan terjadi di dunia cyber***

Iwan Setiawan, ST, MT

heroku.iih@gmail.com

Kategori Cybercrime

1. ***Cyberpiracy***
penggunaan teknologi komputer untuk :
mencetak ulang software atau informasi
mendistribusikan informasi atau software tersebut melalui jaringan komputer
2. ***Cybertrespass***
penggunaan teknologi komputer untuk meningkatkan akses pada:
Sistem komputer sebuah organisasi atau individu
Web site yang di-protect dengan password
3. ***Cyber vandalism***
penggunaan teknologi komputer untuk membuat program yang :
Mengganggu proses transmisi informasi elektronik
Menghancurkan data di komputer

Iwan Setiawan, ST, MT

heroku.iih@gmail.com

Aspek Dari Security

- *Confidentiality*
- *Integrity*
- *Availability*
- Ketiga di atas sering disingkat menjadi **CIA**
- Ada tambahkan lain
 - Non-repudiation
 - Authentication
 - Access Control
 - Accountability

Iwan Setiawan, ST, MT

heroku.iliat@gmail.com

Confidentiality / Privacy

- Kerahasiaan data. Data hanya boleh diakses oleh orang yang berwenang
 - Data-data pribadi
 - Data-data bisnis; daftar gaji, data nasabah
 - Sangat sensitif dalam e-commerce dan healthcare
- Serangan: penyadapan
(teknis dengan sniffer / logger, man in the middle attack; non-teknis dengan social engineering)
- Proteksi: enkripsi

Iwan Setiawan, ST, MT

heroku.iliat@gmail.com

Integrity

- Informasi tidak boleh berubah (tampered, altered, modified) oleh pihak yang tidak berhak
- Serangan
 - Perubahan data oleh orang yang tidak berhak, spoofing
 - Virus yang mengubah berkas
- Proteksi:
 - Message Authentication Code (MAC), digital signature / certificate, hash functions, logging

Iwan Setiawan, ST, MT

heroku.iih@gmail.com

Availability

- Informasi harus tersedia ketika dibutuhkan
- Serangan
 - Meniadakan layanan (Denial of Service / DoS attack) atau menghambat layanan (server dibuat lambat)
- Proteksi
 - Backup, redundancy, DRC, BCP, firewall

Iwan Setiawan, ST, MT

heroku.iih@gmail.com

Non-repudiation

- Tidak dapat menyangkal (telah melakukan transaksi)
 - Menggunakan digital signature
 - Logging

Iwan Setiawan, ST, MT

heroku.iih@gmail.com

Authentication

- Meyakinkan keaslian data, sumber data, orang yang mengakses data, server yang digunakan
 - what you have (identity card)
 - what you know (password, PIN)
 - what you are (biometric identity)
- Serangan: identitas palsu, terminal palsu, situs gadungan

Iwan Setiawan, ST, MT

heroku.iih@gmail.com

Access Control

- Mekanisme untuk mengatur siapa boleh melakukan apa
 - Membutuhkan adanya klasifikasi data:
public, private, confidential, (top)secret
 - Role-based access

Iwan Setiawan, ST, MT

heroku.iih@gmail.com

Accountability

- Dapat dipertanggung-jawabkan
- Melalui mekanisme logging dan audit
- Adanya kebijakan dan prosedur (policy & procedures)

Iwan Setiawan, ST, MT

heroku.iih@gmail.com

Teori Jenis Serangan

- **Interruption**
DoS attack, network flooding
- **Interception**
Password sniffing
- **Modification**
Virus, trojan horse
- **Fabrication**
spoofed packets

The diagram illustrates four types of network attacks using a simple network topology with nodes A and B:

- Interruption:** A vertical bar blocks the direct path from A to B.
- Interception:** A node E is positioned between A and B, with an arrow pointing to the communication line.
- Modification:** Node E is positioned between A and B, with arrows pointing to the communication line from both directions.
- Fabrication:** Node E is positioned between A and B, with an arrow pointing from E to B, representing a spoofed packet.

Iwan Setiawan, ST, MT heroku.iiit@gmail.com

Jenis-Jenis Kejahatan

1. Unauthorized Access ; 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. Contoh *Probing* dan *port*
2. Illegal Contents ; memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum, contohnya adalah penyebaran pornografi.
3. Penyebaran virus secara sengaja
4. Data Forgery ; memalsukan data pada dokumen-dokumen penting yang ada di internet.

Iwan Setiawan, ST, MT heroku.iiit@gmail.com

Jenis-Jenis Kejahatan

5. Cyber Espionage, Sabotage, and Extortion ; 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.
6. Cyberstalking ; mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail dan dilakukan berulang-ulang. (teror)
7. Carding ; mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.

Iwan Setiawan, ST, MT

heroku.iih7@gmail.com

Jenis-Jenis Kejahatan

8. Hacking dan Cracker

Istilah *hacker* ; seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya.

cracker orang yang melakukan aksi-aksi perusakan di internet . Aktivitas cracking ; pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, pelumpuhan target sasaran, DoS (Denial Of Service)- serangan yang bertujuan melumpuhkan target (hang, crash) sehingga tidak dapat memberikan layanan.

Iwan Setiawan, ST, MT

heroku.iih7@gmail.com

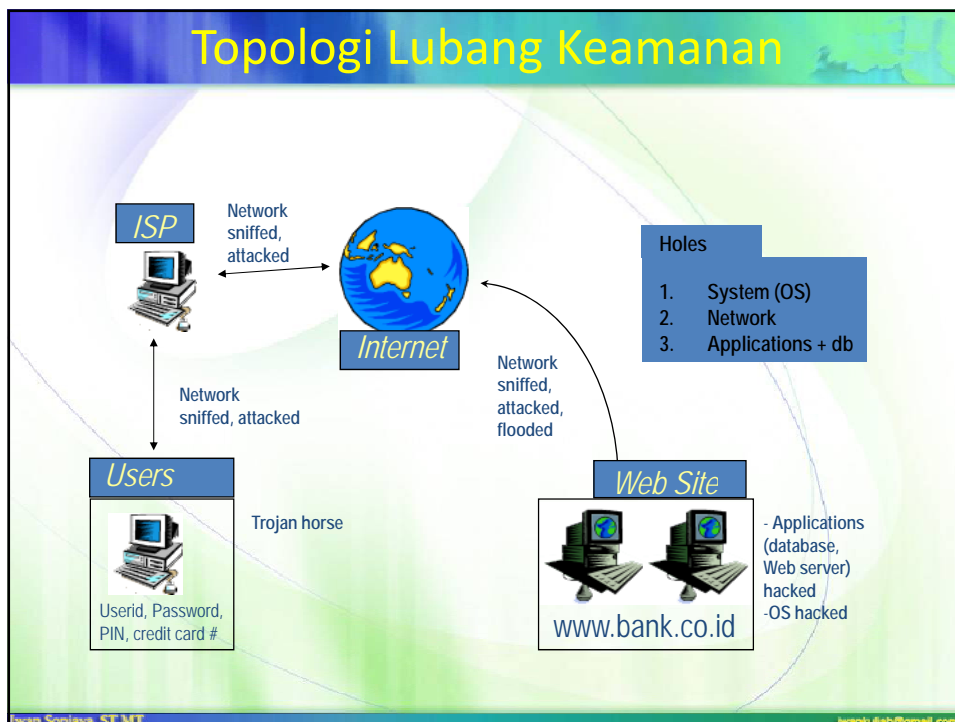
Jenis-Jenis Kejahatan

9. Cybersquatting and Typosquatting
 Cybersquatting ; mendaftarkan domain nama perusahaan orang lain.
 Typosquatting adalah membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain. Nama tersebut merupakan nama domain saingan perusahaan.
10. Hijacking ; pembajakan hasil karya orang lain (pembajakan perangkat lunak).
11. Cyber Terrorism ; mengancam pemerintah atau warganegara, termasuk cracking ke situs pemerintah atau militer.

Iwan Setiawan, ST, MT

herankuliah@gmail.com

Topologi Lubang Keamanan



Iwan Setiawan, ST, MT

herankuliah@gmail.com

CONTOH KASUS - KASUS YANG TERJADI

25

Iwan Setiawan, ST, MT

heroku.iih@gmail.com

Kasus 1 : Nama Domain Mustika Ratu.com

- Kasus Nama Domain (yang pertama di Indonesia) pendaftaran nama Domain Name.
- Mustika Ratu.Com di Amerika tapi digunakan oleh PT Martina Berto, untuk menampilkan produk-produk Belia yang merupakan produk Sari Ayu;
- Tuntutan di dasari tentang Perbuatan Curang dan persaingan Usaha tidak Sehat
- Didakwa pasal 382 KUHP tetapi tidak terbukti secara sah dan meyakinkan, maka terdakwa harus dibebaskan dari dakwaan Kesatu tersebut

Iwan Setiawan, ST, MT

heroku.iih@gmail.com

Kasus 2: Hacker Situs KPU

- Dani yang sebelumnya bekerja di PT Dana Reksa, berhasil menjebol server tnp.kpu.go.id. Dalam aksinya tersebut, Dani berhasil menembus kunci internet protocol PT Dana Reksa. Dan berhasil menembus server KPU.
- Kesalahan : mengacak-acak sejumlah partai yang ikut pemilu dengan mengganti nama-nama partai tersebut. Misalnya, Partai Golkar diganti menjadi Partai Jambu, Partai Demokrat menjadi Partai Mbah Jambon, dan PKS menjadi Partai Kolor Ijo.
- Pengakuan : iseng dan penasaran atas pernyataan pejabat KPU tentang sistem keamanan IT milik KPU tersebut.

Iwan Setiawan, ST, MT

heroku.ili@gnail.com

Kasus 3 : Carding

- Polda Jabar menyerahkan penanganan kasus *carding* yang dilakukan seorang mahasiswa di Bandung, ke Mabes Polri. Pertimbangannya karena kejahatan yang dilakukan tersangka berdampak ke berbagai negara, sehingga pengusutannya membutuhkan keterlibatan pihak Interpol.
- Aksi yang diduga dilakukan Buy alias Sam menyebabkan total kerugian penggunaan kartu kredit orang lain mencapai sekitar DM 15 ribu.
- Terbongkarnya berawal dari teleks Interpol Wiesbaden No 0234203 tertanggal 6 September 2001 yang melaporkan adanya penipuan melalui Internet dan diduga melibatkan seorang WNI yang bertindak sebagai pemesan barang bernama Buy.
- Kepolisian menjerat dengan pasal Pidana (KUHP) soal pencurian dan atau penipuan mengingat perangkat hukum yang lebih tepat, terutama soal *cyberlaw* dan *cybercrime* di Indonesia belum ada.

Iwan Setiawan, ST, MT

heroku.ili@gnail.com

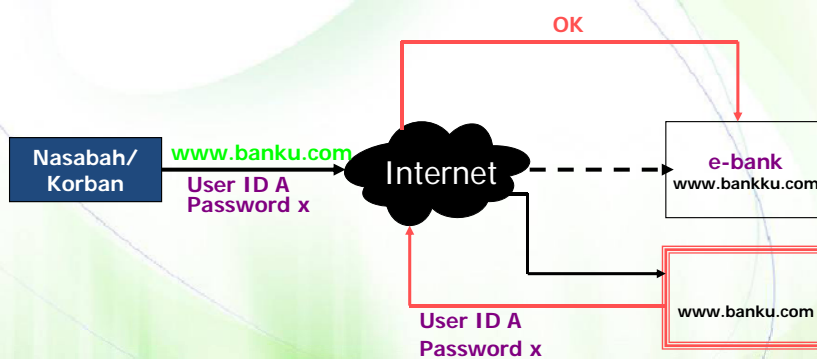
Kasus 4 : Klik BCA

- kasus domain name yang memanfaatkan kesalahan ketik yang mungkin dilakukan oleh nasabah
- Steven Haryanto membeli domain-domain yang serupa www.klikbca.com dimana isi dari tiap situs palsu tersebut sangat mirip dengan situs asli BCA
- kasus typosquatting
 - <http://wwwklikbca.com>
 - <http://www.kilkbca.com>
 - <http://www.clikbca.com>
 - <http://www.klickbca.com>
 - <http://www.klikbac.com>

Iwan Soejaya, ST, MT

heranku.liah@gmail.com

Modus kejahatan : Typo Site



Iwan Soejaya, ST, MT

heranku.liah@gmail.com

Kasus 5: ILoveYou

- Worm, menyebar bulan Mei 2000.
- Pertama kali ditemukan di Filipina
- Ditulis dengan Visual Basic Script, menyebar melalui email dan perpindahan file.
- memiliki attachment "LOVE-LETTER-FOR-YOU.TXT.VBS".
- email memiliki subject "ILOVEYOU"
- Pesan dalam email bertuliskan "kindly check the attached LOVELETTER coming from me."
- Mengirimkan salinan dirinya melalui email ke seluruh alamat yang terdapat di dalam address book dari aplikasi Microsoft Outlook.

Iwan Setiawan, ST, MT

herankuliah@gmail.com

Contoh Kasus: ILoveYou

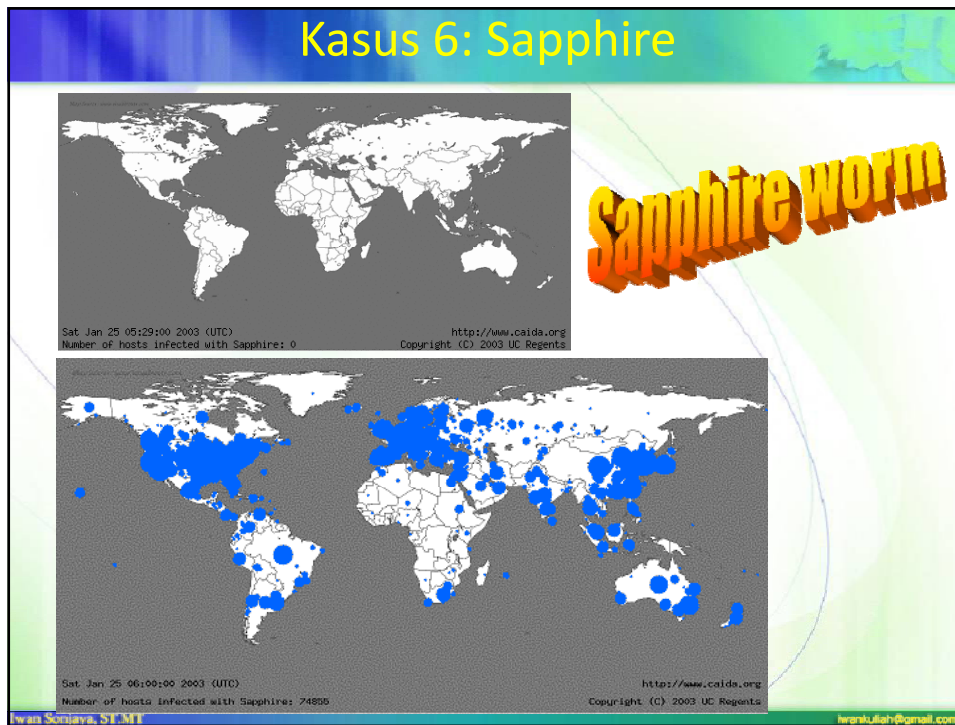
- Ketika dieksekusi, baik melalui pembukaan attachment email maupun file yang telah terinfeksi:
- Mengganti beberapa file tipe tertentu (VisualBasic dan Javascript, WindowsShell ; js, jse, css, wsh, sct, jpg atau jpeg, mp3 atau mp2) dengan salinan dirinya dan membuat melakukan perubahan terhadap file-file tersebut berdasarkan jenisnya yang dilakukan oleh worm adalah menulis ulang (overwrite)

KR/ITHB 2010

32

Iwan Setiawan, ST, MT

herankuliah@gmail.com



Kasus 7: Cyber Terrorism

- Ramzi Yousef, dalang penyerangan pertama ke gedung WTC, diketahui menyimpan detail serangan dalam file yang di enkripsi di laptopnya.
- Osama Bin Laden diketahui menggunakan steganography untuk komunikasi jaringannya.
- Suatu website yang dinamai Club Hacker Muslim diketahui menuliskan daftar tip untuk melakukan hacking ke Pentagon.
- Seorang hacker yang menyebut dirinya sebagai DoktorNuker diketahui telah kurang lebih lima tahun melakukan defacing atau mengubah isi halaman web dengan propaganda anti-American, anti-Israel dan pro-Bin Laden.

Kasus 8 : Vetting

- Vetting ; menyelidiki latar belakang untuk mengetahui rahasia pribadi/karakter(etika)
- Senator Joe Biden, calon presiden partai demokrat th 1987.
- Tuduhan ; menjiplak bagian pidato, dari politikus lain dan melakukan plagiat ketika kuliah di fakultas hukum.

Iwan Setiawan, ST.MT

herakuliah@gmail.com

Kasus 9 : Perilaku tidak Etis dan Ilegal

- Time ; mengubah foto polisi sehingga kesannya lebih mengancam.
- Kasus OJ Simpson ; foto diubah (diperlakukan sebagai alat untuk mencapai tujuan),
- Foto-foto pada suatu produk penurunan berat badan
- Menjual bagian informasi dari database ; data pribadi, riwayat kesehatan, gaji dll.

Iwan Setiawan, ST.MT

herakuliah@gmail.com

Kasus 10 : Phising

- Teknik perampasan account, Via Yahoo Messenger
- pesan biasa namun pada intinya rayuan kepada korban untuk meng-klik alamat situs tertentu (situs jebakan).
- Beberapa alamat yang saat ini paling sering dipakai antara lain www.holiday-picz.com atau summer-picz.com.
- browser Firefox menyediakan fitur peringatan untuk situs- forgery dengan warna merah dan ikon polisi

Iwan Suciyo, ST.MT

heroku.iah@gmail.com

Phising



Dear Citibank user,

Due to database operations some online banking accounts can be lost. We are insisting to our clients to check their account if they are active or if their current balance is right.

Please follow this link and sign on to your online banking account:

https://web.da-us.citibank.com/signin/citifi/scripts/login2/user_setup.jsp

Thank you for using Citibank!

Do not reply to this email.

From: <USBank-Notification-Urgecq@UsBank.com>
 To: ...
 Subject: USBank.com Account Update URGEgb
 Date: Thu, 13 May 2004 17:56:45 -0500

USBank.com

Dear US Bank Customer,

During our regular update and verification of the Internet Banking Accounts, we could not verify your current information. Either your information has been changed or incomplete, as a result your access to use our services has been limited. Please update your information.

To update your account information and start using our services please click on the link below:

<http://www.usbank.com/internetBanking/RequestRouter?requestCmdId=DisplayLoginPage>

Note: Requests for information will be initiated by US Bank Business Development; this process cannot be externally requested through Customer Support.

Iwan Suciyo, ST.MT

heroku.iah@gmail.com

Kasus 11 : PEMBOBOLAN BNI1946 CABANG NEW YORK

- R Demsi karyawan BNI 46 Cabang New York sejak tahun 1980 - September 1986
- pernah bertugas sebagai operator yang terlatih untuk mengoperasikan komputer yang berhubungan dengan City Bank New York untuk meng-entri data dengan memakai password yang berkode RODEMS.
- Pelanggarannya : mentransfer uang (*unauthorized transfer*) milik BNI ke rekening di bank yang lain sejumlah US \$. 9,100,000.- yang terdapat pada Rekening

Iwan Setiawan, ST, MT

heroku.ii@r@gmail.com

Kejahatan Komputer

1. angka *cyber crime* di Indonesia sekitar 30-40 kasus per tahun.
2. penipuan melalui internet, Januari-November 2006, ada 28 kasus penipuan
3. Indonesia menduduki peringkat tertinggi sebagai pelaku *cyber crime* atau kejahatan internet, 90 persennya adalah kejahatan carding atau pemalsuan kartu kredit.

[Badan Reserse Kriminal Kepolisian RI Direktorat II Ekonomi dan Khusus Unit V Infotek-Cyber Crime Komisariss Polisi Idam Wasiadi pada Seminar Nasional Sehari Information Technology Security Rabu, 14 September 2005]

Iwan Setiawan, ST, MT

heroku.ii@r@gmail.com

- Tahun 2002, kejahatan carding 152 dari 155 kasus
- Tahun 2003, kejahatan carding 145 dari 153 kasus
- Tahun 2004 kejahatan carding mencapai 177 dari 192 kasus kejahatan internet.
- Yogyakarta menduduki peringkat tertinggi untuk kasus kejahatan carding, disusul dengan Semarang, Bandung, Jakarta, Medan, Surabaya, dan Riau.

Iwan Setiawan, ST, MT

heroku.iih@gmail.com

Cuplikan statistik kejahatan di dunia

- ▶ **7 Februari 2000 s/d 9 Februari 2000.** Distributed Denial of Service (Ddos) attack terhadap Yahoo, eBay, CNN, Amazon, ZDNet, E-Trade.
- ▶ **2001.** Virus SirCam mengirimkan file dari harddisk korban. File rahasia bisa tersebar. Worm Code Red menyerang sistem IIS kemudian melakukan port scanning dan menyusup ke sistem IIS yang ditemukannya.
- ▶ **2004.** Kejahatan “phising” (menipu orang melalui email yang seolah-olah datang dari perusahaan resmi [bank misalnya] untuk mendapatkan data-data pribadi seperti nomor PIN internet banking) mulai marak

Iwan Setiawan, ST, MT

heroku.iih@gmail.com

Kejahatan ATM



Iwan Soejaya, ST, MT

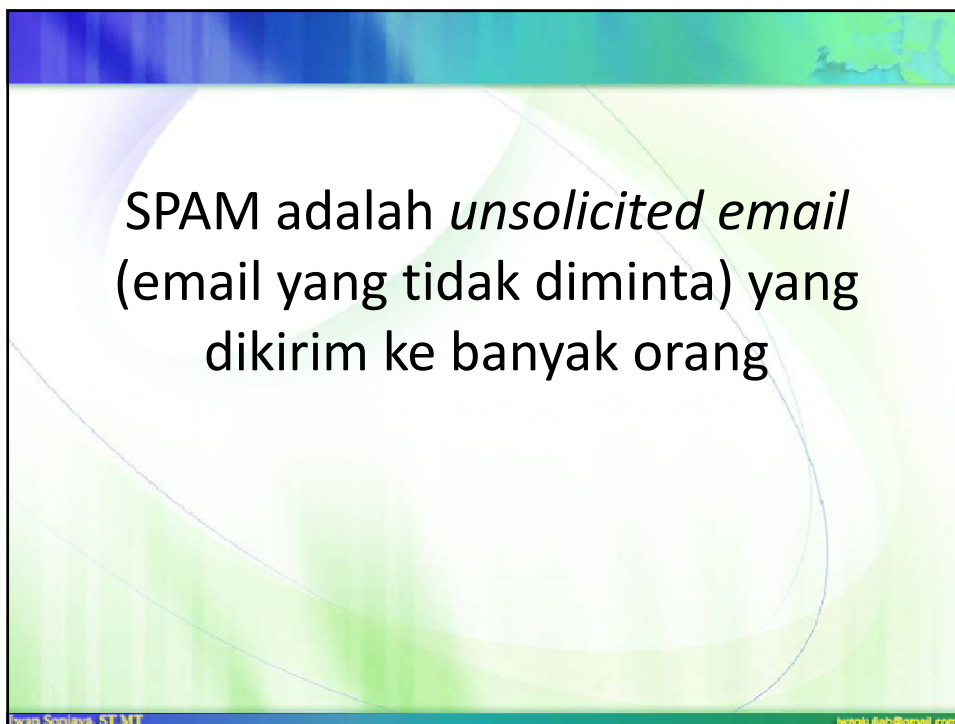
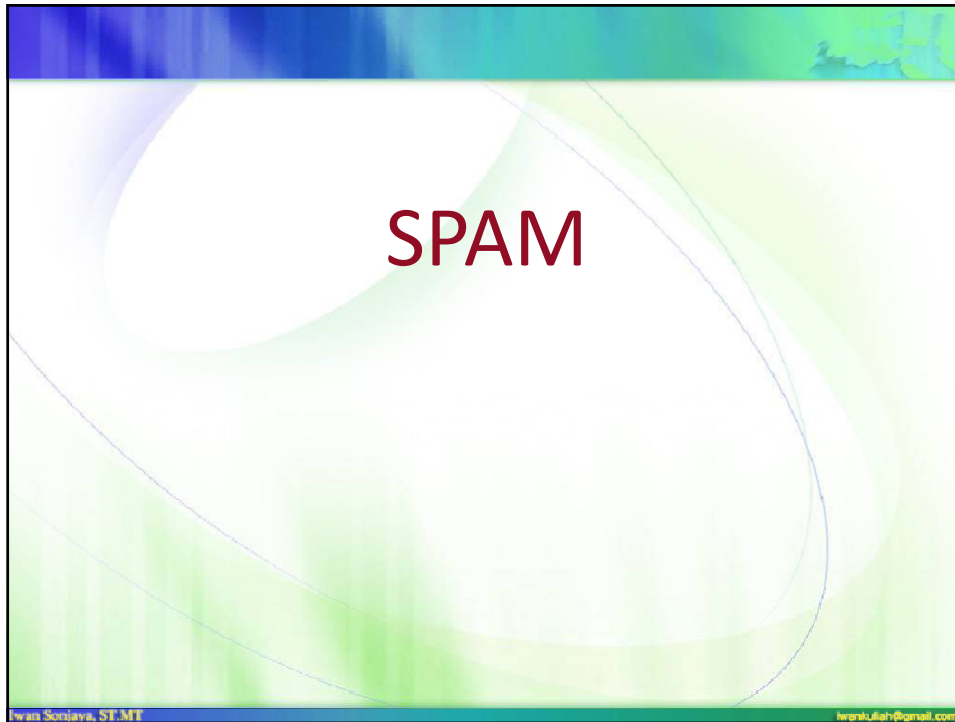
herankuliah@gmail.com



Menyadap PIN dengan wireless camera

Iwan Soejaya, ST, MT

herankuliah@gmail.com



Mailbomb: banyak email ke satu orang

Iwan Soejaya, ST.MT

heroku.iih@gmail.com

- Isi SPAM
 - Iklan, advertensi
 - Tawaran untuk bergabung ke MLM
 - Undian
 - Informasi palsu, phishing
 - Scam, penipuan
 - ...

Iwan Soejaya, ST.MT

heroku.iih@gmail.com

Contoh Spam

From: daniel nando <docdan40@hotmail.fr>
To: docdan40@hotmail.fr
Subject: Dr.Daniel Nando.
Date: Mon, 16 Oct 2006 10:44:40 +0200

Dear Friend,

I am Dr.Daniel Nando. I am a medical doctor in a private hoospital in Abijan Town (Ivory Coast W/Africa). I got your email contact through a chamber of commerce website and will like to explain to you about a Transfer of consignment which I hope you can assist us and which will benefit both of us.

I have a patient, a Sierra Leonian woman who was on admission for some Weeks in my hospital for an ill health. As a matter of fact, one night this woman called my attention and began to tell me her situations, she explained that she had to flee her country with her only son because her late husband a military officer died in a rebel conflict in his country and since then her husbands immediate younger brother had been threatening to eliminate her and the life of her only son because one Certificate of Deposit.

Iwan Setiawan, ST.MT

heroku.iah@gmail.com

Sejarah SPAM

Iwan Setiawan, ST.MT

heroku.iah@gmail.com

- April 1994, *Canter and Siegel* menawarkan jasa mereka untuk “Greencard Lottery” melalui USENET news
 - Usenet news merupakan “bulletin board” atau forum diskusi yang paling populer pada masa itu
 - Jumlah group di Usenet mencapai ribuan dan semua group menerima iklan *Canter and Siegel* itu

Iwan Soejaya, ST.MT

heroku.ii@r@gmail.com

Cerita di belakangnya ...

- Makanan kaleng (daging campur) dari Hormel

Aha! Come on you English, zis is your chance to get your 'ands on somezing reelly special!



Iwan Soejaya, ST.MT

heroku.ii@r@gmail.com

Mengapa Terjadi SPAM?

Iwan Soejaya, ST.MT

heroku.iih@gmail.com

Mengapa Terjadi Spam?

- ***“Ekonomi Internet”*** yang aneh
 - Biaya untuk mengirimkan 1 email sama dengan 1000 email, atau bahkan 1 juta email
 - Sangat murah untuk mengirimkan *unsolicited emails*
 - Berbeda dengan surat biasa, dimana ada biaya untuk mengirimkan *junk mail*

Iwan Soejaya, ST.MT

heroku.iih@gmail.com

Akibat Dari Spam

- Menghabiskan / memboroskan
 - Disk (email storage)
 - Jaringan
 - **Waktu dan produktivitas kerja pengguna**
 - Pengguna tertipu (phising)

Iwan Soejaya, ST, MT

heroku.iih@gmail.com

Hati-hati terhadap Social Engineering

- Mencari informasi rahasia dengan menggunakan teknik persuasif
 - Membujuk melalui telepon dan SMS sehingga orang memberikan informasi rahasia
 - Contoh SMS yang menyatakan menang lotre kemudian meminta nomor PIN

Iwan Soejaya, ST, MT

heroku.iih@gmail.com

Terimakasih.....
Untuk mahasiswa/i yang
tidak ngantuk dan tetap
konsentrasi Mengikuti
Perkuliahan.

