



# Ethical Hacking and Countermeasures

Version 6



## Module II

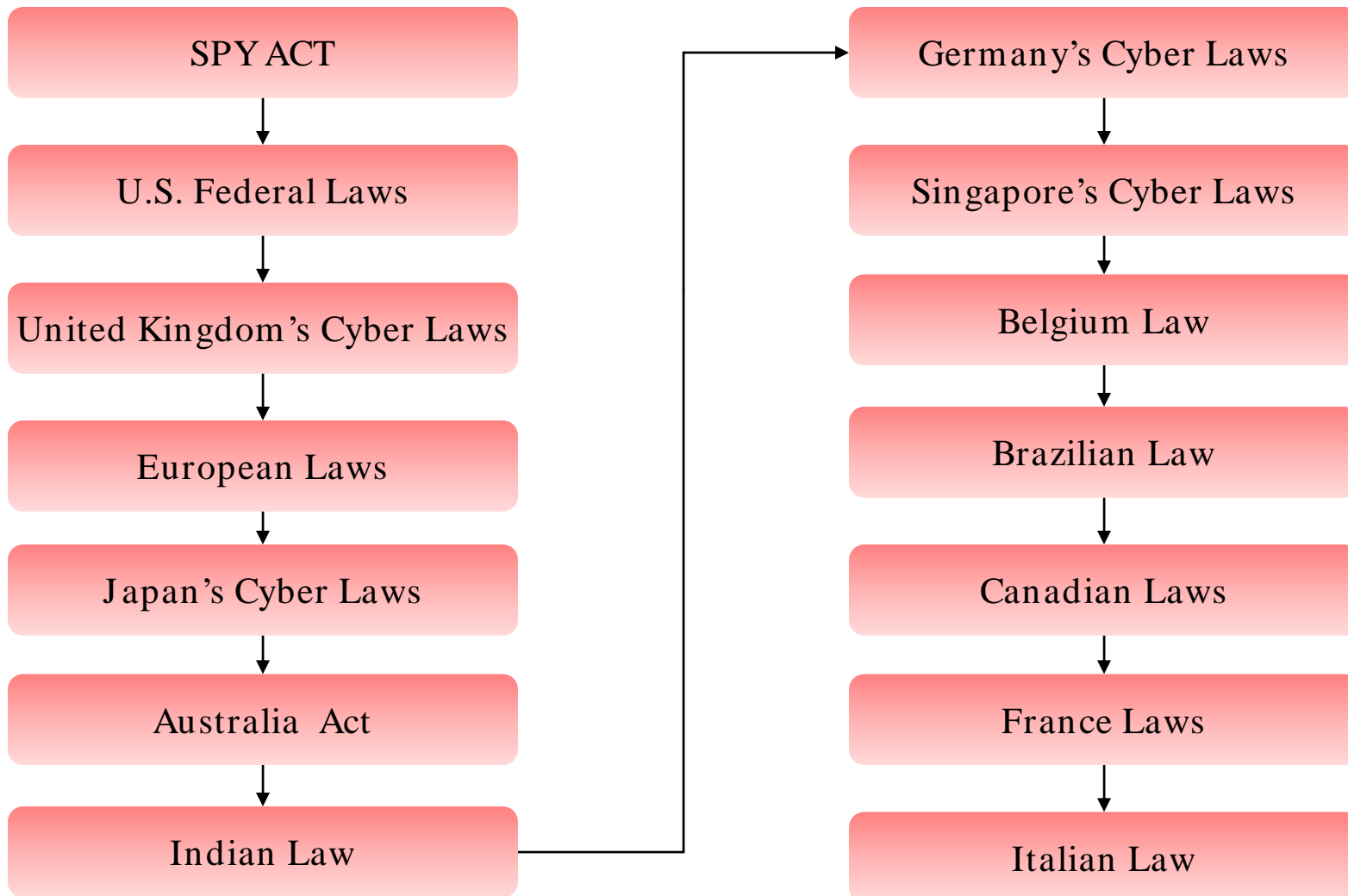
### Hacking Laws

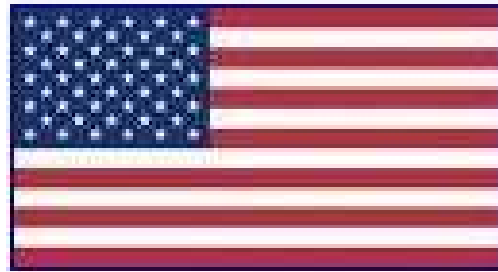
This module will familiarize you with:

- SPY ACT
- U.S. Federal Laws
- United Kingdom's Cyber Laws
- European Laws
- Japan's Cyber Laws
- Australia : The Cybercrime Act 2001
- Indian Law: The Information Technology Act
- Germany's Cyber Laws
- Singapore's Cyber Laws
- Belgium Law
- Brazilian Law
- Canadian Laws
- France Laws
- Italian Law



# Module Flow





# United States

Mission of (USDOJ) United States Department of Justice is to enforce the law and defend the interests of the United States; to ensure public safety against threats foreign and domestic; to provide federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; and to ensure fair and impartial administration of justice for all Americans



The screenshot shows the homepage of the United States Department of Justice. At the top, there is a banner with the American flag and the text "UNITED STATES DEPARTMENT OF JUSTICE" and the DOJ seal. Below the banner is a navigation menu on the left with a search box and links for "ABOUT DOJ", "WHAT WE DO", "PRESS ROOM", "JOBS", "WORKING WITH DOJ", and "RESOURCES". The "RESOURCES" section includes "DOJ AGENCIES" and "DOJ HOME". A yellow "ELEVATED" badge is visible. The main content area features a "Latest News" section with a photo of Attorney General Michael B. Mukasey and a headline: "Remarks Prepared for Delivery by Attorney General Michael B. Mukasey Before the Fraternal Order of Police". The date is "February 25, 2008". Below the headline is a paragraph of text and a "Read More" link. There is also an "Alert About Hoax Emails" section with a warning message and a "Read More" link. At the bottom left, there is a "HIGHLIGHTS" section with a list of links: "Protect America Act", "Performance and Accountability Report 2007", "National Drug Threat Assessment 2008", "Meth Awareness", "The President's DNA Initiative", "Sex Offender Web Site", and "Trafficking in Persons".



## NEWS RELEASE

For Immediate Distribution

February 11, 2008

**Thomas P. O'Brien**

United States Attorney  
Central District of California

Thom Mrozek, Public Affairs Officer  
(213) 894-6947

[thom.mrozek@usdoj.gov](mailto:thom.mrozek@usdoj.gov)  
[www.usdoj.gov/usao/cac](http://www.usdoj.gov/usao/cac)

### **YOUNG 'BOTHERDER' PLEADS GUILTY TO INFECTING MILITARY COMPUTERS AND FRAUDULENTLY INSTALLING ADWARE**

A well-known juvenile member of the "botnet underground" pleaded guilty this afternoon to delinquency charges related to his use of "botnets" – armies of compromised computers – to surreptitiously install adware on computers, including military computers.

A male juvenile – who in court papers is identified as B.D.H., and who used the online nickname "Sobe" – appeared today before United States District Judge Manuel L. Real and entered guilty pleas to two counts of juvenile delinquency. The charges relate to B.D.H. conspiring to commit wire fraud, causing damage to computers used by the federal government in national defense, and accessing protected computers without authorization to commit fraud.



Source: <http://www.usdoj.gov/>

# Securely Protect Yourself Against Cyber Trespass Act (SPY ACT)

## ⊙ SEC. 2. PROHIBITION OF [UNFAIR OR] DECEPTIVE ACTS OR PRACTICES RELATING TO SPYWARE.

- (a) Prohibition- It is unlawful for any person, who is not the owner or authorized user of a protected computer, to engage in unfair or deceptive acts or practices that involve any of the following conduct with respect to the protected computer:
  - (1) Taking control of the computer by--
    - (A) utilizing such computer to send unsolicited information or material from the computer to others;
    - (B) diverting the Internet browser of the computer, or similar program of the computer used to access and navigate the Internet--
      - (i) without authorization of the owner or authorized user of the computer; and
      - (ii) away from the site the user intended to view, to one or more other Web pages, such that the user is prevented from viewing the content at the intended Web page, unless such diverting is otherwise authorized;



# SPY ACT (cont'd)

- (C) accessing, hijacking, or otherwise using the modem, or Internet connection or service, for the computer and thereby causing damage to the computer or causing the owner or authorized user or a third party defrauded by such conduct to incur charges or other costs for a service that is not authorized by such owner or authorized user;
- (E) delivering advertisements that a user of the computer cannot close without undue effort or knowledge by the user or without turning off the computer or closing all sessions of the Internet browser for the computer.
- (2) Modifying settings related to use of the computer or to the computer's access to or use of the Internet by altering--
  - (A) the Web page that appears when the owner or authorized user launches an Internet browser or similar program used to access and navigate the Internet;
  - (B) the default provider used to access or search the Internet, or other existing Internet connections settings;

- (3) Collecting personally identifiable information through the use of a keystroke logging function
- (4) Inducing the owner or authorized user of the computer to disclose personally identifiable information by means of a Web page that--
  - (A) is substantially similar to a Web page established or provided by another person; and
  - (B) misleads the owner or authorized user that such Web page is provided by such other person

## Federal Criminal Code Related to Computer Crime:

- ◉ 18 U.S.C. § 1029. *Fraud and Related Activity in Connection with Access Devices*
- ◉ 18 U.S.C. § 1030. *Fraud and Related Activity in Connection with Computers*
- ◉ 18 U.S.C. § 1362. *Communication Lines, Stations, or Systems*
- ◉ 18 U.S.C. § 2510 et seq. *Wire and Electronic Communications Interception and Interception of Oral Communications*
- ◉ 18 U.S.C. § 2701 et seq. *Stored Wire and Electronic Communications and Transactional Records Access*

## Subsection (a) Whoever -

- (1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;
- (2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating \$1,000 or more during that period;
- (3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;
- (4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;

## Section 1029 (cont'd)

- (5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than \$1,000;
- (6) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of—
  - (A) offering an access device; or
  - (B) selling information regarding or an application to obtain an access device;
- (7) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;

## Section 1029 (cont'd)

- (8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;
- (9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or
- (10) without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device

(A) in the case of an offense that does not occur after a conviction for another offense under this section--

- (i) if the offense is under paragraph (1), (2), (3), (6), (7), or (10) of subsection (a), a fine under this title or imprisonment for not more than 10 years, or both; and
- (ii) if the offense is under paragraph (4), (5), (8), or (9) of subsection (a), a fine under this title or imprisonment for not more than 15 years, or both;

(B) in the case of an offense that occurs after a conviction for another offense under this section, a fine under this title or imprisonment for not more than 20 years, or both; and

(C) in either case, forfeiture to the United States of any personal property used or intended to be used to commit the offense

# Section 1030 – (a) (1)

Subsection (a) Whoever--

- (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;



# Section 1030 (2) (A) (B) (C)

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

- (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
- (B) information from any department or agency of the United States; or
- (C) information from any protected computer if the conduct involved an interstate or foreign communication;

## Section 1030 (3) (4)

- (3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;
- (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;

# Section 1030 (5) (A) (B)

(5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(5)(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--

## Section 1030 (5) (B) (cont'd)

- (i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;
- (ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
- (iii) physical injury to any person;
- (iv) a threat to public health or safety; or
- (v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

## Section 1030 (6) (7)

- (6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--
- (A) such trafficking affects interstate or foreign commerce; or
  - (B) such computer is used by or for the Government of the United States;
- (7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

- (1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
- (B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
- (2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

## Penalties (cont'd)

- ◉ (B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if-
  - (i) the offense was committed for purposes of commercial advantage or private financial gain;
  - (ii) the offense was committed in furtherance of any criminal or tortuous act in violation of the Constitution or laws of the United States or of any State; or
  - (iii) the value of the information obtained exceeds \$5,000;
- ◉ (C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(3)(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and



## Communication Lines, Stations, or Systems

### Law is applicable if:

- Person willfully injures or destroys any of the works, property, or material of any means of communication
- Maliciously obstructs, hinders, or delays the transmission of any communication

### Penalty:

- A fine or imprisonment for not more than 10 years, or both



- ◉ Trafficking in counterfeit label for phone records, copies of computer programs or computer program documentation or packaging, and copies of motion pictures or other audio visual works, and trafficking in counterfeit computer program documentation or packaging
  - Law is applicable if :
    - Person knowingly traffics in a counterfeit label affixed or designed to be affixed
    - Intentionally traffics in counterfeit documentation or packaging for a computer program
  - Penalty:
    - Fined or imprisoned for not more than five years, or both



## Trademark Offenses

- ⊙ Trafficking in counterfeit goods or services
  - Law is applicable if:
    - Person intentionally traffics or attempts to traffic in goods or services
    - Knowingly uses a counterfeit mark
  - Penalty:
    - Fined not more than \$2,000,000 or imprisoned not more than 10 years, or both



## Trade Secret Offenses

- ◉ *Economic espionage*

- Law is applicable if:
  - Person knowingly steals or without authorization obtains a trade secret
  - Without authorization copies or transmits a trade secret
  - Receives, buys, or possesses a trade secret
- Penalty:
  - Fined not more than \$10,000,000



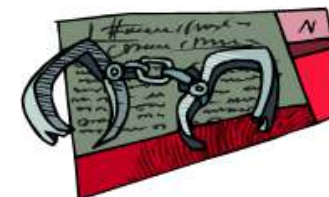
- ◉ *Unauthorized publication or use of communications*

- Practices prohibited

- Receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio
- Intercepting any radio communication and divulging or publishing the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person
- Scrambling of Public Broadcasting Service programming

- Penalty:

- Fined not more than \$2,000 or imprisoned for not more than 6 months, or both



## Computer trespass in the first degree

(1) A person is guilty of computer trespass in the first degree if the person, without authorization, intentionally gains access to a computer system or electronic database of another; and

(a) The access is made with the intent to commit another crime;  
or

(b) The violation involves a computer or database maintained by a government agency

(2) Computer trespass in the first degree is a class C felony

[1984 c 273 § 1.]

Source: <http://apps.leg.wa.gov/>

## **815.02 Legislative intent--**The Legislature finds and declares that:

- (1) Computer-related crime is a growing problem in government as well as in the private sector
- (2) Computer-related crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime
- (3) The opportunities for computer-related crimes in financial institutions, government programs, government records, and other business enterprises through the introduction of fraudulent records into a computer system, the unauthorized use of computer facilities, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets are great

(4) While various forms of computer crime might possibly be the subject of criminal charges based on other provisions of law, it is appropriate and desirable that a supplemental and additional statute be provided which proscribes various forms of computer abuse

## **815.04 Offenses against intellectual property; public records exemption--**

(1) Whoever willfully, knowingly, and without authorization modifies data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or network commits an offense against intellectual property

(2) Whoever willfully, knowingly, and without authorization destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property



# Florida: § 815.01 to 815.07 (cont'd)

(3)(a) Data, programs, or supporting documentation which is a trade secret as defined in s. 812.081 which resides or exists internal or external to a computer, computer system, or computer network which is held by an agency as defined in chapter 119 is confidential and exempt from the provisions of s. 119.07(1) and s. 24(a), Art. I of the State Constitution

(b) Whoever willfully, knowingly, and without authorization discloses or takes data, programs, or supporting documentation which is a trade secret as defined in s. 812.081 or is confidential as provided by law residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property

(4)(a) Except as otherwise provided in this subsection, an offense against intellectual property is a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084

(b) If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084

**815.05 Trade secret information**--The Legislature finds that it is a public necessity that trade secret information as defined in s. 812.081, and as provided for in s. 815.04(3), be expressly made confidential and exempt from the public records law because it is a felony to disclose such records. Due to the legal uncertainty as to whether a public employee would be protected from a felony conviction if otherwise complying with chapter 119, and with s. 24(a), Art. I of the State Constitution, it is imperative that a public records exemption be created. The Legislature in making disclosure of trade secrets a crime has clearly established the importance attached to trade secret protection. Disclosing trade secrets in an agency's possession would negatively impact the business interests of those providing an agency such trade secrets by damaging them in the marketplace, and those entities and individuals disclosing such trade secrets would hesitate to cooperate with that agency, which would impair the effective and efficient administration of governmental functions. Thus, the public and private harm in disclosing trade secrets significantly outweighs any public benefit derived from disclosure, and the public's ability to scrutinize and monitor agency action is not diminished by nondisclosure of trade secrets

## **815.06 Offenses against computer users--**

(1) Whoever willfully, knowingly, and without authorization:

(a) Accesses or causes to be accessed any computer, computer system, or computer network;

(b) Disrupts or denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another;

(c) Destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network;

(d) Destroys, injures, or damages any computer, computer system, or computer network; or

(e) Introduces any computer contaminant into any computer, computer system, or computer network, commits an offense against computer users.

(2)(a) Except as provided in paragraphs (b) and (c), whoever violates subsection (1) commits a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(b) Whoever violates subsection (1) and:

1. Damages a computer, computer equipment, computer supplies, a computer system, or a computer network, and the monetary damage or loss incurred as a result of the violation is \$5,000 or greater;
2. Commits the offense for the purpose of devising or executing any scheme or artifice to defraud or obtain property; or
3. Interrupts or impairs a governmental operation or public communication, transportation, or supply of water, gas, or other public service, commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084

(c) Whoever violates subsection (1) and the violation endangers human life commits a felony of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084

- (3) Whoever willfully, knowingly, and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network commits a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083
- (4) (a) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, computer equipment, computer supplies, or computer data may bring a civil action against any person convicted under this section for compensatory damages  
(b) In any action brought under this subsection, the court may award reasonable attorney's fees to the prevailing party
- (5) Any computer, computer system, computer network, computer software, or computer data owned by a defendant which is used during the commission of any violation of this section or any computer owned by the defendant which is used as a repository for the storage of software or data obtained in violation of this section is subject to forfeiture as provided under ss. 932.701-932.704.

- (6) This section does not apply to any person who accesses his or her employer's computer system, computer network, computer program, or computer data when acting within the scope of his or her lawful employment
- (7) For purposes of bringing a civil or criminal action under this section, a person who causes, by any means, the access to a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in both jurisdictions



## IC 35-43-1-4 Computer tampering

Sec. 4. (a) As used in this section:

"Computer network" and "computer system" have the meanings set forth in IC 35-43-2-3.

"Computer program" means an ordered set of instructions or statements that, when executed by a computer, causes the computer to process data.

"Data" means a representation of information, facts, knowledge, concepts, or instructions that:

- (1) may take any form, including computer printouts, magnetic storage media, punched cards, or stored memory;
- (2) has been prepared or is being prepared; and
- (3) has been processed, is being processed, or will be processed; in a computer system or computer network.

Source: <http://www.in.gov/>

Sec. 4. (b) A person who knowingly or intentionally alters or damages a computer program or data, which comprises a part of a computer system or computer network without the consent of the owner of the computer system or computer network commits computer tampering, a Class D felony. However, the offense is a:

- (1) Class C felony if the offense is committed for the purpose of terrorism; and
- (2) Class B felony if the offense is committed for the purpose of terrorism and results in serious bodily injury to a person.

*As added by P.L.35-1986, SEC.2. Amended by P.L.156-2001, SEC.11*



## IC 35-43-2-3 Computer trespass

(a) As used in this section "Access" means to:

- (1) approach;
- (2) instruct;
- (3) communicate with;
- (4) store data in;
- (5) retrieve data from; or
- (6) make use of resources of a computer, computer system, or computer network

through:

- (1) remote terminals;
- (2) a complex consisting of two (2) or more interconnected computers; or
- (3) a worldwide collection of interconnected networks operating as the Internet

(b) A person who knowingly or intentionally accesses:

- (1) a computer system;
- (2) a computer network; or
- (3) any part of a computer system or computer network;

without the consent of the owner of the computer system or computer network, or the consent of the owner's licensee, commits computer trespass, a Class A misdemeanor

# Federal Managers Financial Integrity Act of 1982

- ⊙ Sec.1. This Act may be cited as the "Federal Managers' Financial Integrity Act of 1982".
- ⊙ Sec.2. Section 113 of the Accounting and Auditing Act of 1950 (31 U.S.C.66a) is amended by adding at the end thereof the following new subsection:
  - (d) (1) (A) To ensure compliance with the requirements of subsection (a)(3) of this section, internal accounting and administrative controls of each executive agency shall be established in accordance with standards prescribed by the Comptroller General, and shall provide reasonable assurances that—
    - (i) obligations and costs are in compliance with applicable law
    - (ii) funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation

- ◉ § 552. Public information; agency rules, opinions, orders, records, and proceedings
  - (a) Each agency shall make available to the public information as follows:
    - (1) Each agency shall separately state and currently publish in the Federal Register for the guidance of the public--
      - (A) descriptions of its central and field organization and the established places at which, the employees (and in the case of a uniformed service, the members) from whom, and the methods whereby, the public may obtain information, make submittals or requests, or obtain decisions;
      - (B) statements of the general course and method by which its functions are channeled and determined, including the nature and requirements of all formal and informal procedures available;
      - (C) rules of procedure, descriptions of forms available or the places at which forms may be obtained, and instructions as to the scope and contents of all papers, reports, or examinations;
      - (D) substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency; and
      - (E) each amendment, revision, or repeal of the foregoing.

Source: <http://www.usdoj.gov>

Copyright © by **EC-Council**

# Federal Information Security Management Act (FISMA)

- Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), requires each Federal agency to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The information security program must include—
  - Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;

# Federal Information Security Management Act (FISMA) (cont'd)

- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system;
- Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;
- Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the agency) of the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks;
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (including the management, operational, and technical controls of every agency information system identified in their inventory) to be performed with a frequency depending on risk, but no less than annually;

# Federal Information Security Management Act (FISMA) (cont'd)

- A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures and practices of the agency;
- Procedures for detecting, reporting, and responding to security incidents (including mitigating risks associated with such incidents before substantial damage is done and notifying and consulting with the Federal information security incident response center, and as appropriate, law enforcement agencies, relevant Offices of Inspector General, and any other agency or office, in accordance with law or as directed by the President; and
- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

### ◉ § 552a. Records maintained on individuals

- (b) Conditions of disclosure

No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be--

- (1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;
- (2) required under section 552 of this title;
- (3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;
- (4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of Title 13;
- (5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

# The Privacy Act Of 1974

## 5 U.S.C. § 552a (cont'd)

- (6) to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value;
- (7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;
- (8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;
- (9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;
- (10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office;
- (11) pursuant to the order of a court of competent jurisdiction; or
- (12) to a consumer reporting agency in accordance with section 3711(e) of Title 31.



## ⊙ Section 202 Authority to Intercept Voice Communications in Computer Hacking Investigations

- *Previous law*: Under previous law, investigators could not obtain a wiretap order to intercept wire communications (those involving the human voice) for violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030).
- *Amendment*: Section 202 amends 18 U.S.C. § 2516(1) – the subsection that lists those crimes for which investigators may obtain a wiretap order for wire communications – by adding felony violations of 18 U.S.C. § 1030 to the list of predicate offenses.

## ◉ Section 209 Obtaining Voice-mail and Other Stored Voice Communications

- *Previous law:* Under previous law, the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2703 et seq., governed law enforcement access to stored electronic communications (such as e-mail), but not stored wire communications (such as voice-mail). Instead, the wiretap statute governed such access because the definition of "wire communication" (18 U.S.C. § 2510(1)) included stored communications, arguably requiring law enforcement to use a wiretap order (rather than a search warrant) to obtain unopened voice communications. Thus, law enforcement authorities used a wiretap order to obtain voice communications stored with a third party provider but could use a search warrant if that same information were stored on an answering machine inside a criminal's home.
- Regulating stored wire communications through section 2510(1) created large and unnecessary burdens for criminal investigations. Stored voice communications possess few of the sensitivities associated with the real-time interception of telephones, making the extremely burdensome process of obtaining a wiretap order unreasonable.

# Government Paperwork Elimination Act (GPEA)

## Section 1. What GPEA policies should agencies follow?

The Government Paperwork Elimination Act (GPEA) requires Federal agencies, by October 21, 2003, to provide individuals or entities the option to submit information or transact with the agency electronically and to maintain records electronically when practicable. GPEA specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form. It also encourages Federal government use of a range of electronic signature alternatives.

Sections 1703 and 1705 of GPEA charge the Office of Management and Budget (OMB) with developing procedures for Executive agencies to follow in using and accepting electronic documents and signatures, including records required to be maintained under Federal programs and information that employers are required to store and file with Federal agencies about their employees. These procedures reflect and are to be executed with due consideration of the following policies:

# Government Paperwork Elimination Act (GPEA) (cont'd)

- maintaining compatibility with standards and technology for electronic signatures generally used in commerce and industry and by State governments;
- not inappropriately favoring one industry or technology;
- ensuring that electronic signatures are as reliable as appropriate for the purpose in question;
- maximizing the benefits and minimizing the risks and other costs;
- protecting the privacy of transaction partners and third parties that have information contained in the transaction;
- ensuring that agencies comply with their recordkeeping responsibilities under the FRA for these electronic records. Electronic record keeping systems reliably preserve the information submitted, as required by the Federal Records Act and implementing regulations; and
- providing, wherever appropriate, for the electronic acknowledgment of electronic filings that are successfully submitted.

## ⦿ Section 2. What GPEA Procedures Should Agencies Follow?

- GPEA recognizes that building and deploying electronic systems to complement and replace paper-based systems should be consistent with the need to ensure that investments in information technology are economically prudent to accomplish the agency's mission, protect privacy, and ensure the security of the data. Moreover, a decision to reject the option of electronic filing or record keeping should demonstrate, in the context of a particular application and upon considering relative costs, risks, and benefits given the level of sensitivity of the process, that there is no reasonably cost-effective combination of technologies and management controls that can be used to operate the transaction and sufficiently minimize the risk of significant harm. Accordingly, agencies should develop and implement plans, supported by an assessment of whether to use and accept documents in electronic form and to engage in electronic transactions. The assessment should weigh costs and benefits and involve an appropriate risk analysis, recognizing that low-risk information processes may need only minimal consideration, while high-risk processes may need extensive analysis.

# Government Paperwork Elimination Act (GPEA) (cont'd)

- Performing the assessment to evaluate electronic signature alternatives should not be viewed as an isolated activity or an end in itself. Agencies should draw from and feed into the interrelated requirements of the Paperwork Reduction Act, the Privacy Act, the Computer Security Act, the Government Performance and Results Act, the Clinger-Cohen Act, the Federal Managers' Financial Integrity Act, the Federal Records Act, and the Chief Financial Officers Act, as well as OMB Circular A-130 and Presidential Decision Directive 63.
- The assessment should develop strategies to mitigate risks and maximize benefits in the context of available technologies, and the relative total costs and effects of implementing those technologies on the program being analyzed. The assessment also should be used to develop baselines and verifiable performance measures that track the agency's mission, strategic plans, and tactical goals, as required by the Clinger-Cohen Act.
- In addition to serving as a guide for selecting the most appropriate technologies, the assessment of costs and benefits should be designed so that it can be used to generate a business case and verifiable return on investment to support agency decisions regarding overall programmatic direction, investment decisions, and budgetary priorities. In doing so, agencies should consider the effects on the public, its needs, and its readiness to move to an electronic environment.



# Mexico

The portal to the government of Mexico includes general information about Mexico and its government agencies

It also covers the following topics: education, democracy, employment, health, sports, culture, national security, environment, foreign relations, transportation, immigration, family, agriculture, tourism, business, and housing.





The screenshot shows the homepage of the Mexican government's official website. At the top left is the logo for 'MÉXICO GOBIERNO DE LA REPÚBLICA' with the national coat of arms. The main header features the URL 'www.gob.mx' and the text 'Portal Ciudadano Sitio Oficial del Gobierno de México'. On the right side, there are utility links for 'English', 'Envía tus comentarios', 'Mapa de sitio', 'Inicio', 'Versión para imprimir', 'gob.mx móvil', and 'RSS'. Below the header is a horizontal navigation menu with buttons for 'Ciudadanos', 'Negocios', 'Extranjeros', 'Servidores Públicos', and 'Turismo'. Underneath this is a secondary menu with 'Temas', 'Grupos', and 'Trámites y Servicios'. A large banner image of a smiling woman is positioned on the right side of the page. Below the banner, the date and time are displayed: 'Hoy es jueves 28 de febrero de 2008 | 5:40:26 p.m. GMT-6'. To the right of the date is a 'Cambiar color' section with options for 'AZUL', 'GRIS', and 'BLANCO'. A breadcrumb trail reads 'Tú estás aquí: Inicio > Ciudadanos > Temas'. The main content area is divided into two columns. The left column is titled 'Derechos del ciudadano' and contains a sub-header 'Conoce los acuerdos, las organizaciones y los derechos humanos' followed by a list of links: 'Cultura política', '¿Qué son los derechos humanos?', 'Jóvenes y sus derechos', 'Organizaciones de defensa de los Derechos Humanos', and 'Acuerdos, tratados y legislación sobre Derechos Humanos'. The right column is titled 'Educación' and contains a sub-header 'Consulta la educación por niveles, las instituciones, los tipos de educación, las becas y apoyos que el gobierno tiene para ti' followed by a list of links: 'Becas y apoyo educativo', 'Bibliotecas y libros en línea', 'Instituciones educativas', 'Educación por niveles', and 'Profesores'. At the bottom of the right column is a section titled 'Gobierno Federal'. On the far right, there is a search bar labeled 'Buscador', a button for 'Escríbele al Presidente' with the presidential seal, and a vertical menu with links for 'Gobierno de la A a la Z', 'Leyes Federales', 'Leyes Estatales', 'Pregúntale al Gobierno', and 'Trámites y Servicios más comunes' with 'CURP' listed below.

## **Section 30-45-5 — Unauthorized computer use**

A person who knowingly, willfully and without authorization, or having obtained authorization, uses the opportunity the authorization provides for purposes to which the authorization does not extend, directly or indirectly accesses, uses, takes, transfers, conceals, obtains, copies or retains possession of any computer, computer network, computer property, computer service, computer system or any part thereof, when the

- damage to the computer property or computer service has a value of two hundred fifty dollars (\$250) or less, is guilty of a petty misdemeanor;
- damage to the computer property or computer service has a value of more than two hundred fifty dollars (\$250) but not more than five hundred dollars (\$500), is guilty of a misdemeanor;

Source: <http://law.justia.com/>

- damage to the computer property or computer service has a value of more than five hundred dollars (\$500) but not more than two thousand five hundred dollars (\$2,500), is guilty of a fourth degree felony;
- damage to the computer property or computer service has a value of more than two thousand five hundred dollars (\$2,500) but not more than twenty thousand dollars (\$20,000), is guilty of a third degree felony;
- damage to the computer property or computer service has a value of more than twenty thousand dollars (\$20,000), is guilty of a second degree felony





Brazil

Justiça Federal - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.jf.gov.br/

Inicial | Links | Mapa do Portal

## Portal da Justiça Federal

"Todos são iguais perante a lei."

sexta-feira, 22 de fevereiro de 2008

Pesquisa Unificada

- Superior Tribunal de Justiça
- Conselho da Justiça Federal
- Justiça Federal
- Turma Nacional de Uniformização dos JEFs
- Serviços de Informação
- Central de Atendimento ao Juiz Federal
- Publicações
- Ensino
- Certificados Digitais
- Imprensa
- Rede Ibero-Americana

### TNU não admite incidente do INSS e mantém correção monetária em licença maternidade requerida após o parto

Por não apresentar julgados do Superior Tribunal de Justiça com semelhança fática aos fatos do acórdão da Primeira Turma Recursal da Seção Judiciária da Bahia, o presidente da Turma Nacional de Uniformização da Jurisprudência dos Juizados Especiais Federais (TNU), ministro Gilson Dipp, não admitiu incidente de uniformização ajuizado pelo INSS contra decisão que concedeu correção monetária a salário-maternidade requerido fora do prazo legal pela segurada.

[leia mais...](#)

### Juízes da Colômbia reconhecem sucesso da experiência dos juizados especiais brasileiros

A entrada em funcionamento, no dia 1º de fevereiro deste ano, dos primeiros juizados especiais criminais na Colômbia e o reconhecimento do êxito da experiência brasileira neste campo levaram o Conselho Superior da Judicatura daquele país a enviar delegação de juízes para conhecer de perto o funcionamento dos juizados especiais federais. Recebidos na manhã desta quinta-feira (21) pelo coordenador da Justiça Federal, ministro Gilson Dipp, os juízes colombianos José Alfredo Escobar, Núbia Ângela Burgos Diaz, Luis Fernando Contreras e Carlos Moreno realizam programa de visitas que inclui conhecer o funcionamento dos juizados especiais federais.

[leia mais...](#)

### Aposentadoria especial é regida pela lei vigente à época da atividade

O segurado que prestou serviço em condições especiais tem direito à aposentadoria especial e à conversão do tempo de serviço especial em comum nos termos da legislação vigente à época em que realizada a atividade. O entendimento da Turma Nacional de Uniformização da Jurisprudência dos Juizados Especiais Federais (TNU) baseou a decisão de seu presidente, ministro Gilson Dipp, ao admitir e determinar a devolução de incidente de uniformização de

#### Consultas


- Certidão Negativa
- Acompanhamento processual
- Jurisprudência Unificada
- Biblioteca do CEJ
- Atos Normativos Institucionais
- Bibliografia da Justiça Federal
- Estatísticas da Justiça Federal
- Tabelas e Manual de Cálculos
- Programa de Gestão Documental
- MoReq-Jus - Versão 1

#### Eventos

- Workshop - Comunicação Institucional na Sociedade da Informação

Done McAfee SiteAdvisor

## Brazil has become a trailblazer in computer use.

Source: 

Publication Date: 25-SEP-05

Byline: Jack Chang

Sep. 25--RIO DE JANEIRO, Brazil -- While Brazilians live with levels of poverty and violence that mark them as Third World citizens, they are emerging as trailblazers in the kind of high technology that's propelling many First World economies.

Evolving fields such as open-source software, online banking and social networking through the Internet are finding a welcome home in this nation of more than 180 million people. So are legions of sophisticated hackers, who regularly make international headlines with their exploits.

That combination of high-tech savvy and lawlessness has pushed Brazil to the front line of some of the hottest technology debates, such as those over intellectual property rights and corporate control of media.

It also has placed the country in the crosshairs of media companies fighting losing battles against pirated wares.

On the economic front, Brazilians have yet to build an information technology industry on par with those in other developing countries such as India and Malaysia.

But this Latin American giant is coming up with new uses for technology, many of them...

Source: <http://www.accessmylibrary.com/>

## ◉ ENTRY OF FALSE DATA INTO THE INFORMATION SYSTEM

- Art. 313-A. Entry, or facilitation on the part of an authorized employee of the entry, of false data, improper alteration or exclusion of correct data with respect to the information system or the data bank of the Public Management for purposes of achieving an improper advantage for himself or for some other person, or of causing damages

## ◉ Penalty-imprisonment for 2 to 12 years, and fines

## ◉ UNAUTHORIZED MODIFICATION OR ALTERATION OF THE INFORMATION SYSTEM

- Art. 313-B. Modification or alteration of the information system or computer program by an employee, without authorization by or at the request of a competent authority

## ◉ Penalty-detention for 3 months to 2 years, and fines

Source: <http://www.mosstingrett.no/>



Canada



This website provides all the source of consolidated Acts and regulations of Canada

The Canadian Legal Information Institute (CanLII) is a not-for-profit organization launched by the Federation of Law Societies of Canada with the goal of making primary sources of Canadian law accessible at no charge on the Internet. CanLII gathers legislative and judicial texts, as well as legal commentaries, from federal, provincial and territorial jurisdictions on a single Web site.





|                              |                            |  |                                      |                             |
|------------------------------|----------------------------|--|--------------------------------------|-----------------------------|
| <a href="#">Français</a>     | <a href="#">Contact us</a> | <a href="#">Help</a>                     | <a href="#">Search</a>               | <a href="#">Canada Site</a> |
| <a href="#">Justice Home</a> | <a href="#">Site Map</a>   | <a href="#">Programs and Initiatives</a> | <a href="#">Proactive Disclosure</a> | <a href="#">Laws</a>        |

SERVING CANADIANS 

- [The Minister and Attorney General](#)
- [The Department](#)
- [Programs](#)
- [NewsRoom](#)
- [Corporate Publications](#)
- [A-Z Index](#)
- [Justice and the Law](#)
- [For Youth](#)
- [Work Opportunities](#)

Welcome to the Department of Justice Canada



**Featuring...**  
[Justice and the Law](#)  
 This page contains links to information about the Canadian legal system.  
[More Features](#)

**What's New**

February 22, 2008

[Minister of Justice Refers Murder Conviction to New Brunswick Court of Appeal](#)

Backgrounder: [Application for Ministerial Review](#)

[Special Advocates for Bill C-3 \(Security Certificates under the Immigration and Refugee Protection Act\)](#)

February 21, 2008

[Government of Canada Announces Transitional Housing Support for Toronto Drug Treatment Courts](#)

Backgrounder: [Drug Treatment Courts](#)

Backgrounder: [National Anti-Drug Strategy](#)

**Most Visited Sites**

- [Child Support](#)
- [Family Violence](#)
- [Parenting After Divorce](#)
- [Policy Centre for Victim Issues](#)
- [Recruitment](#)
- [Research and Statistics](#)
- [Youth Justice](#)

**In the News**

- [Special Advocates](#)
- [Office of the Director of Public Prosecutions](#)
- [Financial Assistance for Victims to Attend National Parole Board](#)



## Quebec police bust alleged hacker ring

17 raids nabbed suspects in a dozen towns across Quebec

**Jan Ravensbergen, Canwest News Service**

Published: Thursday, February 21, 2008

Allen McInnis/Canwest News Service MONTREAL -- Quebec provincial police said Wednesday they have dismantled what they called the largest and most damaging computer-hacking network ever uncovered in Canada.

During several action-packed early-morning hours Wednesday, provincial police and RCMP officers dismantled the latest hacking ring by successfully carrying out 17 lightning-fast raids in 12 towns small and large across Quebec, including Montreal.

They collared 17 hacking suspects aged 17 to 26. All are male except for one, a 19-year-old woman.

Some of the suspects were to appear in court Wednesday while others were released with the promise to appear.

Police raiding parties also sealed and carted away dozens of hard drives and other computer components from the homes of each of the suspects.

This hardware is believed to contain the smoking guns -- a bonanza of incriminating data to document the alleged ring, said SQ Capt. Frederick Gaudreau, lead investigator.

"This is a new form of organized crime," he proclaimed to reporters summoned to SQ headquarters in Montreal.

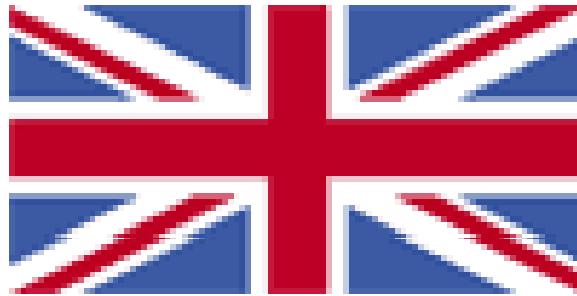
Savvy youngsters who've grown up with computers can take advantage of lax or inattentive users connected via broadband to the Internet.



Source: <http://www.nationalpost.com/>

- ◉ Canadian Criminal Code Section 342.1 states:
- ◉ (1) Every one who, fraudulently and without color of right,
  - (a) obtains, directly or indirectly, any computer service,
  - (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly , any function of a computer system
  - (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system
- ◉ Person to commit an offence under paragraph (a), (b) or (c) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years

Source: <http://www.mosstingrett.no/>



# United Kingdom

OPSI(Office of Public Sector Information) provides the full text of all UK Parliament Public General Acts (from 1988 onwards) and all Local Acts (from 1991 onwards) as they were originally enacted.

Acts of the UK Parliament - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://www.opsi.gov.uk/acts.htm

Office of PUBLIC SECTOR INFORMATION

the national archives

About OPSI | Contact Us | FAQs | Sitemap | A - Z Site Index | Glossary | Viewing Advice

You are here:  
Home > Legislation > Original > UK > Acts >

Last Updated: 20/02/2008

**Acts of the UK Parliament and Explanatory Notes**

This page provides links to the full text of all UK Parliament Public General Acts (from 1988 onwards) and all Local Acts (from 1991 onwards) **as they were originally enacted.**

Some legislation made prior to 1988 has been added as PDF where available. Prior to 1988 legislation was not produced electronically, but all legislation before this date is still available in its original print format from The Stationery Office Ltd.

**Public Acts**

**1988 - present**

All UK Parliament Public General Acts from 1988 onwards in HTML and PDF

2008 | 2007 | 2006 | 2005 | 2004 | 2003 | 2002 | 2001 | 2000 | 1999 | 1998 | 1997 | 1996 | 1995 | 1994 | 1993 | 1992 | 1991 | 1990 | 1989 | 1988

Search:

Advanced Search Search

**Related Pages**

- > What are Explanatory Notes?
- > Search Legislation
- > Tracking Legislation

**External Websites**

- > Buy Legislation
- > United Kingdom Parliament
- > Northern Ireland Assembly
- > Scottish Parliament

The screenshot shows a Microsoft Internet Explorer browser window displaying the Office of Public Sector Information (OPSI) website. The address bar shows the URL: [http://www.opsi.gov.uk/acts/acts1990/Ukpga\\_19900018\\_en\\_1.htm](http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm). The page header includes the OPSI logo and navigation links such as "About OPSI", "Contact Us", "FAQs", "Sitemap", "A - Z Site Index", "Glossary", and "Viewing Advice". The main content area features the Royal Coat of Arms and the title "Computer Misuse Act 1990 (c. 18)" followed by "1990 CHAPTER 18" and "ARRANGEMENT OF SECTIONS". A "Go to Preamble" link is visible at the bottom. The right sidebar contains a search box, "Legislation Views" (Plain Version, Single Page Version), "Why keep printing? Go green. Buy your official copy...", "Related Pages" (Copyright Guidance Note on the Re-Use of Legislation), and "Feeds" (Computer Misuse Act 1990, Acts of UK Parliament). The left sidebar lists various legislative categories like "Legislation", "New", "Original", "UK", "Acts", "Local Acts", "Statutory Instruments", "Church Measures", "Northern Ireland", "Scotland", "Wales", "Revised", "Chronological Tables", "Public Sector Information", "Click-Use Licensing", "Information Asset Register", "Information Fair Trader Scheme", and "Official Publications".

## Obeying New U.K. Hack-Attack Law to Cost Banks Millions.

Source: → Knight Ridder/Tribune Business News

Publication Date: 22-APR-04

By Pete Warren, Evening Standard, London Knight Ridder/Tribune Business News

Apr. 22--Britain's banks are being forced to reveal potentially damaging details about how often they have been attacked by computer hackers.

New international banking laws mean financial institutions must be more open about their vulnerability to IT-related risks, including so-called cyber attacks, so their insurers and auditors can gauge their liability.

The new openness demanded by the Basel II regulations looks set to cost the industry hundreds of millions of pounds as banks set up databases detailing a minimum of three years of hack attacks.

Banks will have to pass the information to their insurance companies and auditors, and to international regulators from 2007, so they must set up systems to log and monitor attacks from now on.

Complying with the rules will cost the average-sized British bank an estimated UKpound 200 million over the next five years.

Traditionally reluctant to tell outside organisations about security matters for reasons of commercial secrecy, and in some cases simple embarrassment, banks have been bitterly opposed to this new legislation.

The very existence of attacks by cyber-criminals is one of the industry's best-kept secrets, much to the frustration of police.

However, banks that do not comply with the new laws will be obliged to set aside 2.8 percent of their assets to meet any IT-related liability -- and that would be unthinkable in the current competitive climate.

John Sherwood of business consultancy ID Risk says: "Capital allocated against risk is dead money as far as a bank is concerned because they are not using it to make money."

He believes most, if not all, UK banks are already working to meet the 2007 deadline.

Indeed, a spokeswoman at Lloyds TSB confirmed it had started to compile a database of computer security incidents to comply with the demands.



Source: <http://www.accessmylibrary.com/>



## Computer Misuse Act 1990

- (1) A person is guilty of an offense if-
  - (a) he causes a computer to perform any function with the intent to secure access to any program or data held in any computer,
  - (b) the access he intends to secure is unauthorized, and
  - (c) he knows at the time when he causes the computer to perform the function that that is the case
- (2) The intent a person has to have to commit an offense under this section need not to be directed at:
  - (a) any particular program or data,
  - (b) a program or data of any particular kind, or
  - (c) a program or data held in any particular computer
- (3) A person guilty of an offense under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both

# United Kingdom's Cyber Laws (cont'd)

- (4) A person is guilty of an offense under this section if he commits an offense under section 1 above (" the unauthorized access offense") with intent
  - (a) to commit an offense to which this section applies; or
  - (b) to facilitate the commission of such an offense and the offense he intends to commit or facilitate is referred to below in this section as the further offense
- (5) This section applies to offences
  - (a) for which the sentence is fixed by law; or
  - (b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years
- (6) It is immaterial for the purposes of this section whether the further offense is to be committed on the same occasion as the unauthorized access offense or on any future occasion
- (7) A person may be guilty of an offense under this section even though the facts are such that the commission of the further offense is impossible

- (8) A person guilty of an offense under this section shall be liable
- (a) on summary conviction, to imprisonment for a term not exceeding the statutory maximum or to both; and
  - (b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both
- (9) A person is guilty of an offense if -
- (a) he does any act which causes an unauthorized modification of the contents of any computer; and -
  - (b) at the time when he does the act he has the requisite intent and the requisite knowledge.
- (10) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any and by so doing -
- (a) to impair the operation of any computer;
  - (b) to prevent or hinder access to any program or data held in any computer;
  - or
  - (c) to impair the operation of any such program or the reliability of any such data

## Unauthorized access to computer material

- (1) In the Computer Misuse Act 1990 (c. 18) (“the 1990 Act”), section 1 (offence of unauthorized access to computer material) is amended as follows.
- (2) In subsection (1)—
  - (a) in paragraph (a), after “any computer” there is inserted “, or to enable any such access to be secured”;
  - (b) in paragraph (b), after “secure” there is inserted “, or to enable to be secured,”.
- (3) For subsection (3) there is substituted—

“(3) A person guilty of an offence under this section shall be liable—

  - (a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

Source: <http://www.opsi.gov.uk/>

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.”

## **Making, supplying or obtaining articles for use in computer misuse offences**

After section 3 of the 1990 Act there is inserted—

### **“3A Making, supplying or obtaining articles for use in offence under section 1 or 3**

(1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1 or 3.

(2) A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1 or 3.

# Police and Justice Act 2006 (cont'd)

(3) A person is guilty of an offence if he obtains any article with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 1 or 3.

(4) In this section “article” includes any program or data held in electronic form.

(5) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.”



# Europe

This site provides user-friendly fact sheets which summarize EU legislation. The fact sheets are divided into 32 subject areas which are the Activities of the European Union. You will find not only summaries of existing measures, but also a follow-up of legislative proposals in policies as diverse as External Relations and Employment and Social Affairs. With almost 2,500 fact sheets updated daily, the coverage of legislation is comprehensive and up-to-date





## Conforming European hacking laws. (Tech Talk).(Brief Article)

Source:  Security Management

Publication Date: 01-JUN-03

By the end of this year, European Union countries must adopt coordinated but still-to-be-determined anti-hacking regulations. Under a recent "Framework Decision" by the Council of the European Union (the European Community's legislative body), member states must "establish the criminal offence of illegal access to information systems." Some countries may already be in compliance with that requirement. For example, the U.K.'s Computer Misuse Act defines computer crimes such as virus introduction in great detail.

But another goal of the decision is to provide hacking penalties "which are effective, proportionate and dissuasive." These penalties are notoriously different throughout Europe. For example, a virus writer who released last year's Gokar worm received a two-year sentence under the U.K. law, while the Netherlands-based creator of the Kournikova e-mail worm received 150 hours of community service.

The Council of Europe's Cybercrime Convention, another European initiative aimed at harmonizing cybercrime laws between European countries, covers similar ground but is still far from being ratified. That convention, which has been signed by nations (including the United States), still needs to be ratified by five countries (including three member states) before it goes into force. So far, according to the most recently available information, only one country--Albania--has ratified the treaty.

---

Source: <http://www.accessmylibrary.com/>

- ◉ SECTION 1 - SUBSTANTIVE CRIMINAL LAW
- ◉ According to this law, following are considered as offences:
  - Title 1 - Offences against the confidentiality, integrity and availability of computer data and systems
  - Article 2 - Illegal Access
    - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right
  - Article 3 - Illegal Interception
  - Article 4 - Data Interference
    - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right

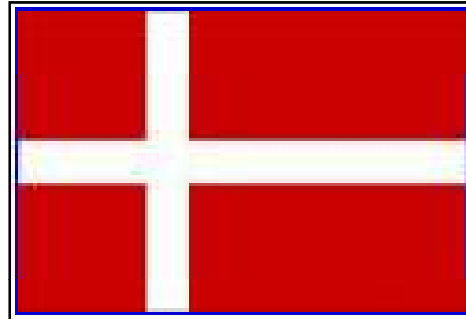


Belgium

- ◉ COMPUTER HACKING
- ◉ Article 550(b) of the Criminal Code:
  - ◉ § 1. Any person who, aware that he is not authorised, accesses or maintains his access to a computer system, may be sentenced to a term of imprisonment of 3 months to 1 year and to a fine of (Bfr 5,200-5m) or to one of these sentences
  - ◉ If the offence specified in § 1 above is committed with intention to defraud, the term of imprisonment may be from 6 months to 2 years
  - ◉ § 2. Any person who, with the intention to defraud or with the intention to cause harm, exceeds his power of access to a computer system, may be sentenced to a term of imprisonment of 6 months to 2 years and to a fine of (Bfr 5,200-20m) or to one of these sentences

Source: <http://www.mosstingrett.no/>

Copyright © by **EC-Council**



Denmark

This site provides the information about **MINISTRY OF JUSTICE**

The Ministry handles tasks relating to the entire judicial system, including the police service, the Office of the Public Prosecutor, the legal system, and the prison and probation services

The Ministry is also responsible for legislation pertaining to the law of persons and family law, and legislation pertaining to securities and data protection.



**MINISTRY OF FOREIGN AFFAIRS OF DENMARK**  
DENMARK.DK

Type in search words

NEWS SUBSCRIBE CONTACT LINKS SITEMAP FRANÇAIS DEUTSCH ESPAÑOL


ABOUT DENMARK VISIT DENMARK LIVE AND WORK STUDY IN DENMARK BUSINESS LOUNGE DENMARK ABROAD

Home > About Denmark > Government & Politics > Danish Ministries > Ministry of Justice

Print Subscribe Send


## MINISTRY OF JUSTICE

The Ministry handles tasks relating to the entire judicial system, including the police service, the Office of the Public Prosecutor, the legal system, and the prison and probation services. The Ministry is also responsible for legislation pertaining to the law of persons and family law, and legislation pertaining to securities and data protection.



**LINKS**

- > Ministry of Justice
- > Data Protection Agency



Original URL: [http://www.theregister.co.uk/2007/08/02/cycling\\_email\\_hack/](http://www.theregister.co.uk/2007/08/02/cycling_email_hack/)

## Man cuffed over 'cycling cheat' email hack

By [John Leyden](#)

Published Thursday 2nd August 2007 18:42 GMT

A man suspected of hacking into the emails of controversial Danish cyclist Michael Rasmussen in a bid to look for dirt has been arrested in Denmark.

The 30-year suspect, who can't be named for legal reasons, allegedly broke into Rasmussen's account in a hunt for evidence of his whereabouts at the time of missed drug tests. The alleged perp tried to sell these emails to Danish regional paper *BT*, the *AP* [reports](#) ([http://news.yahoo.com/s/ap/20070802/ap\\_on\\_sp\\_ot/cyc\\_rasmussen\\_hacker](http://news.yahoo.com/s/ap/20070802/ap_on_sp_ot/cyc_rasmussen_hacker)).

*BT* said it was approached by a man offering to sell Rasmussen's e-mail inbox on Monday. The miscreant told the paper he broke into the account after guessing the rider's password. After contacting Rasmussen and confirming that he owned the the account the paper contacted police.

Officers subsequently raided the suspect's home in Herning, western Denmark. They seized computers and charged the suspect with computer hacking offences, punishable on conviction by up to 18 months imprisonment.

Rasmussen was fired by his Rabobank team and subsequently removed from the Tour de France - while leading the grueling race - over allegations that he lied about his whereabouts in order to evade drug testing. The climbing specialist missed random drug tests in May and June. A retired professional rider said he saw Rasmussen in Italy during June at a time when the Dane claimed he was half way across the world in Mexico.

The accusations came to a head on 25 July, shortly after Rasmussen won a mountain stage to virtually ensure his overall win of the 2007 Tour de France four days before its conclusion in Paris, when he was fired by his Rabobank team. Spain's Alberto Contador subsequently won the Tour. ®



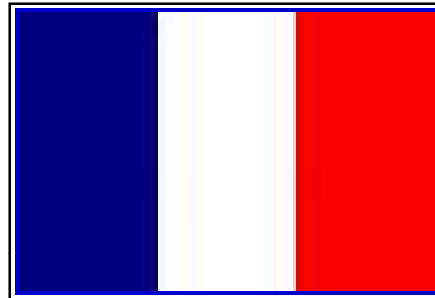
Source: <http://www.theregister.co.uk/>



## ⦿ Penal Code Section 263:

- (2) Any person who, in an unlawful manner, obtains access to another persons information or programs which are meant to be used in a data processing system, shall be liable to a fine, to simple detention or to imprisonment for a term not exceeding 6 months
- (3) If an act of the kind described in subsection 1 or 2 is committed with the intent to procure or make oneself acquainted with information concerning trade secrets of a company or under other extraordinary aggravating circumstances, the punishment shall be increased to imprisonment for a term not exceeding 2 years

Source: <http://www.mosstingrett.no/>



France

This is an official website for Legal laws in France. These legal rules can be adopted by States or between States, on a national level, but they can also come from national and international case-law.

The screenshot shows the Legifrance website interface. At the top left is the French Republic logo with the motto 'Liberté • Égalité • Fraternité'. The main header features the 'Legifrance.gouv.fr' logo and the tagline 'LE SERVICE PUBLIC DE LA DIFFUSION DU DROIT'. The date 'Thursday, February 28, 2008' is displayed in the top right. Below the header, there is a news section titled 'Actualité' with two bullet points: 'LOI n° 2008-175 du 26 février 2008 facilitant l'égal accès des femmes et des hommes au mandat de conseiller général' and 'LOI n° 2008-174 du 26 février 2008 relative à la rétention de sûreté et à la...'. The main content area is divided into several sections: 'Sites juridiques' (Assemblées parlementaires, Juridictions, etc.), 'Droit français' (Lois et règlements, Conventions collectives, Jurisprudence), 'Droit européen', and 'Droit international'. A search bar is present in the 'Lois et règlements' section. On the right side, there are additional sections: 'Le Journal officiel de la République française', 'Actualité juridique', and 'Qualité de la réglementation'.

## Rogue French Trader Accused of Hacking

By PIERRE-ANTOINE SOUCHARD — Jan 27, 2008

PARIS (AP) — Societe Generale detailed Sunday how a young trader evaded all its controls to bet some \$73 billion — more than the French bank's market worth — on European markets, saying he hacked computers and used other "fraudulent methods" to cover his tracks, causing billions in losses.

The bank says the trader, Jerome Kerviel, did not appear to have profited personally from the transactions and seemingly worked alone — a version of events reiterated Sunday by Jean-Pierre Mustier, chief executive of the bank's corporate and investment banking arm. But, in a conference call with reporters, Mustier added: "I cannot guarantee to you 100 percent that there was no complicity."

French judicial officials, speaking on condition of anonymity because the investigation is continuing, said Kerviel can be held until Monday afternoon. The trader was taken into custody on Saturday and under French law, he must either be released or handed preliminary charges after 48 hours in custody.

Societe Generale said Kerviel misappropriated other people's computer access codes, falsified documents and employed other methods to cover his tracks — helped by his previous experience working in offices that monitor traders.

THIS IS A BREAKING NEWS UPDATE. Check back soon for further information. AP's earlier story is below.

PARIS (AP) — A young trader blamed for losses that cost France's Societe Generale more than \$7 billion hacked computers and used "several techniques of fraud," the bank said Sunday, as judicial officials said the man would remain in custody a further 24 hours.

In a five-page document, Societe Generale also sought to counter the notion that it had disrupted markets by unwinding the massive positions built up by the 31-year-old trader. The bank took three days last week to sell off the contracts on the Eurostoxx, DAX and FTSE indices, but said that it had done so in a "controlled" way.

French judicial officials, speaking on condition of anonymity because the investigation is continuing, said Jerome Kerviel can be held until Monday afternoon. Kerviel was taken into custody on Saturday.

Under French law, after 48 hours in custody, he must either be released or handed preliminary charges.

Societe Generale said Kerviel misappropriated other people's computer access codes, falsified documents and employed other methods to cover his tracks — helped by his previous experience working in offices that monitor traders.

"He had a very good understanding of all of Societe Generale's processing and control procedures," the statement said.



Source: <http://ap.google.com>

- ◉ Chapter III: ATTACKS ON SYSTEMS FOR AUTOMATED DATA PROCESSING
- ◉ Article 323-1:
  - The act of fraudulently gaining access to, or maintaining, in all or part of an automated data processing system is punishable by imprisonment not exceeding one year and a fine of up to 100.000 F
- ◉ Article 323-2:
  - The act of hindering or of distorting the functioning of an automated data processing system is punishable by imprisonment not exceeding three years and a fine up to 300.000 FF

Source: <http://www.mosstingrett.no/>



Germany

This is an German website for Federal Ministry of Justice,, is responsible for legal policy and has the central task of upholding the German constitutional state. In the BMJ new laws are prepared, and existing ones are amended or repealed.

The screenshot shows the website interface for the German immigration portal. On the left is a vertical navigation menu with categories like 'Immigration in the past', 'Immigration today', and 'Immigration for the future'. The main content area features a large photo of a diverse group of people in a professional setting. Below the photo, there are sections for 'Immigration in the past', 'Immigration today', and 'Immigration for the future'. A text block explains the Immigration Act, and there are links to 'Specifics of the Immigration Act' (PDF, 80 KB). Other visible elements include 'Modern Nationality Law' and 'Publication' sections.

Original URL: [http://www.theregister.co.uk/2007/08/13/german\\_anti-hacker\\_law/](http://www.theregister.co.uk/2007/08/13/german_anti-hacker_law/)

## Germany enacts 'anti-hacker' law

By [John Leyden](#)

Published Monday 13th August 2007 15:15 GMT

Germany has introduced draconian anti-hacker measures that criminalise the creation or possession of dual-use security tools.

An update to the country's computer hacking laws makes denial of service attacks and hacking assaults against individuals clearly criminal. Gaining access to data, without necessarily stealing information, would also become an arrestable offence. The most serious offences are punishable on conviction by up to 10 years' imprisonment.

Controversy centres around provision in the laws that make it an offense to create or distribute "hacking tools", a notoriously ambiguous term. The distinctions between, for example, a password cracker and a password recovery tool, or a utility designed to run DOS attacks and one designed to stress-test a network, are not covered by the new law, critics argue. Possession of dual-use tools - port scanners such as nmap or security scanners like nessus - is punishable by imprisonment of up to 12 months and a fine.

The changes in German computer hacking law are similar to measures proposed in the UK's Police and Justice Bill, which were dropped following industry pressure.

The effects of Germany's anti-hacker crusade are already beginning to bite. Security tools developers have already begun packing up shop, security consultancy [Sünnet Beskerming reports](#)

([http://www.beskerming.com/commentary/2007/08/12/249/German\\_Security\\_Professionals\\_in\\_the\\_Mist](http://www.beskerming.com/commentary/2007/08/12/249/German_Security_Professionals_in_the_Mist)

For example, the developers of KisMAC, an OS X wireless network scanning tool, have stopped development in Germany and are in the process of [moving](#) (<http://kismac.de>) to the Netherlands. Proof-of concept exploit code that accompanied the Month of PHP bugs project, developed by German coder Stefan Esser, has been [withdrawn](#) (<http://blog.php-security.org/archives/91-MOPB-Exploits-taken-down.html>)



Source: <http://www.theregister.co.uk/>



⊙ Penal Code Section 202a. Data Espionage:

- (1) Any person who obtains without authorization, for himself or for another, data which are not meant for him and which are specially protected against unauthorized access, shall be liable to imprisonment for a term not exceeding three years or to a fine
- (2) Data within the meaning of subsection 1 are only such as are stored or transmitted electronically or magnetically or in any form not directly visible

⊙ Penal Code Section 303a: Alteration of Data

- (1) Any person who unlawfully erases, suppresses, renders useless, or alters data (section 202a(2)) shall be liable to imprisonment for a term not exceeding two years or to a fine
- (2) The attempt shall be punishable



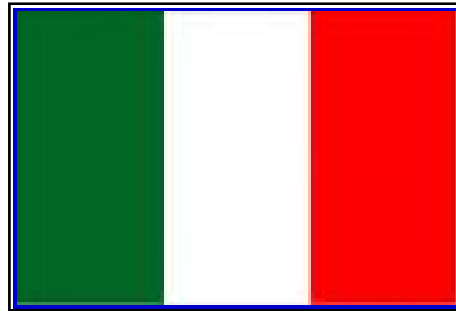
Greece

## ⦿ Criminal Code Article 370C § 2:

- Every one who obtains access to data recorded in a computer or in the external memory of a computer or transmitted by telecommunication systems shall be punished by imprisonment for up to three months or by a pecuniary penalty not less than ten thousands drachmas
- If the act concerns the international relations or the security of the State, he shall be punished according to Art. 148



Source: <http://www.mosstingrett.no/>



Italy

- ◉ Penal Code Article 615 ter: Unauthorized access into a computer or telecommunication systems:
  - Anyone who enters unauthorized into a computer or telecommunication system protected by security measures, or remains in it against the expressed or implied will of the one who has the right to exclude him, shall be sentenced to imprisonment not exceeding three years
  - The imprisonment is from one until five years
  - if the crime is committed by a public official or by an officer of a public service, through abuse of power or through violation of the duties concerning the function or the service, or by a person who practices - even without a licence - the profession of a private investigator, or with abuse of the capacity of a system operator



Netherland

## The Netherlands adopts cybercrime pact

From...



November 30, 2000  
Web posted at: 10:56 a.m. EST (1556 GMT)

by Joris Evers

(IDG) -- The Netherlands is adopting an international treaty to ease crime fighting in cyberspace even before the treaty has been signed.

The Dutch Department of Justice told members of Parliament on Tuesday that Dutch law needs to be changed to be in accordance with the crime in cyberspace treaty. The treaty is still in draft and has various stages to go before signing, which is expected to take place late next year.

"The Netherlands wants to show the way," said Peter Csonka, deputy head of the division of economic crime at the Council of Europe in Strasbourg, France. "It's the first time I've heard about an amendment process being put in place."

The Council of Europe, which groups together 41 European nations and also includes the U.S., Canada and Japan, is the entity drafting the treaty.

Law enforcement in the Netherlands will have broader authority after the amendments to the law are accepted. Internet service providers (ISPs) will have to save customers' Internet traffic data once requested by the police, the Dutch Justice minister said in a letter to Parliament. A request will have to be based on suspicion.

Companies are also affected. The new law will force network managers to cooperate with the authorities in tapping network traffic. Companies will not be asked to make their networks ready for tapping, which ISPs are required to do.

Action against attacks on computer networks is also taken. It will become illegal to sell passwords and access codes and providing tools clearly meant to damage networks. Such tools would be computer viruses or hacking programs.

Source: <http://archives.cnn.com/>

- ◉ Criminal Code Article 138 a:

- Any person who intentionally and unlawfully accesses an automated system for the storage or processing of data, or part of such a system, shall be liable, as guilty of breach of computer peace, to term of imprisonment not exceeding six months or a fine of 10.000 guilders if he:
  - (a). Breaks through a security system, or
  - (b) obtains access by a technical intervention, with the help of false signals or a false key or by acting in a false capacity







Norway

This U.S. Embassy website is a guide to a broad range of information about Norway. The guide includes references to internet resources as well as information about commercial online databases, print resources, and institutions and/or specialists who can provide further information on a given topic.

United States Embassy, Norway

SEARCH

EMBASSY SERVICES | ABOUT THE USA | **ABOUT NORWAY** | INFORMATION RESOURCE CENTER

Home > About Norway

### ABOUT NORWAY


This section of the U.S. Embassy website is a guide to a broad range of information about Norway, much of it in English. The guide includes references to internet resources as well as information about commercial online databases, print resources, and institutions and/or specialists who can provide further information on a given topic. People who intend to live in Norway for a shorter or more extended period of time might find it useful to read the U.S. State Department's "Post Report" on Norway. Post Reports are written for U.S. Government employees and family members assigned to diplomatic missions abroad and provide information about living, housing, and health conditions, as well as recreational, cultural, and employment opportunities for family members in the host country. If you cannot find what you're looking for in our web pages, please contact the **Information Resource Center** at [pubaffoslo\[at\]sign\]gmail.com](mailto:pubaffoslo[at]sign]gmail.com) and we will help you as best we can. (But please read our [notice about email policy](#) before contacting us)

|                |                     |                   |
|----------------|---------------------|-------------------|
| General        | Foreign Relations   | Literature        |
| Arts & Culture | Government/Politics | News/Media        |
| Business       | Genealogy/Biography | Norwegian America |
| Education      | History             | Statistics        |
| Employment     | Law                 | Travel            |
| Entertainment  | Libraries/Archives  |                   |

Henrik Ibsens gate 48, 0244 Oslo, Norway - switchboard (47) 22 44 85 50

Printer Friendly

## Norwegian Acquitted in Digital Media Case.(Jon Lech Johansen)(Brief Article)

Source:  The Online Reporter

Publication Date: 11-JAN-03

An Oslo tribunal consisting of a judge and two technical experts acquitted Jon Lech Johansen, now 19, of charges that he trifled with copyright law by making a program called DeCSS available that enabled users to break the CSS copy-protection code that's meant to prevent DVDs from being copied.

Norway has laws outlawing hacking and computer piracy but nothing like the American Digital Millennium Copyright Act (DMCA).

Johansen was attempting to convert a DVD he had purchased from one format to another. When he made the code available for doing so to others, he was hauled into court.

Now the Oslo court has found that "someone who buys a DVD film that has been legally produced has legal access to the film. Something else would apply if the film had been an illegal, pirate copy. Consumers' rights to legally obtained DVDs apply even if the films are played in a different way than the makers had foreseen."

The MPAA filed a complaint with the Norwegian legal authorities in January 2000, charging that the then 17-year-old Johansen with economic crimes. If convicted, he could have spent two years in prison and been fined. The prosecutors haven't said whether they'll appeal.

Johansen told the Associated Press he was "very satisfied. I had figured that we could win, but it can go either way."

The motion picture industry developed CSS to encrypt DVDs and make them piracy-proof, then pushed for the American Congress to pass laws, such as the DMCA, that made it illegal to crack anti-piracy encryption or publish the hack. There are other CSS de-scrambling programs floating around the web so more lawsuits are to be expected.

However, after verdicts in the two big headline European anti-piracy cases, the media companies are still looking for a win that side of the pond. Last spring they lost an attempt to shut down the Kazaa peer-to-peer network in the Dutch courts. In the two big headline American copyright trials, Napster and Madster, the media companies were victorious. The third, which will probably be the biggest of them all in terms of legal impact and publicity, has begun and pits the major media players against Kazaa founders Niklas Zennstrom and Janus Friis Degnbol, Sharman Networks, Streamcast Networks, Grokster, La Galiote BV and Indigo Investment.



Source: <http://www.accessmylibrary.com/>

Copyright © by **EC-Council**

All Rights Reserved. Reproduction is Strictly Prohibited

## **Penal Code § 145:**

Any person who unlawfully opens a letter or other closed document or in a similar manner gains access to its contents, or who breaks into another persons locked depository shall be liable to fines or to imprisonment for a term not exceeding 6 months

The same penalty shall apply to any person who unlawfully obtains access to data or programs which are stored or transferred by electronic or other technical means.

If damage is caused by the acquisition or use of such unauthorized knowledge, or if the felony is committed for the purpose of obtaining for any person an unlawful gain, imprisonment for a term not exceeding 2 years may be imposed

Accomplices shall be liable to the same penalty

Public prosecution will only be instituted when the public interest so requires

Source: <http://www.cybercrimelaw.net/>

## **Penal Code § 145b:**

Any person who unlawfully makes available a computer password or similar data, by which the whole or any part of a computer system is capable of being accessed, shall be sentenced for spreading of access data, to a fine or imprisonment not exceeding 6 months or both.

Serious spreading of access data shall be sentenced to imprisonment not exceeding 2 years. In deciding whether the spreading is serious, special regard shall be paid to whether the data may access sensitive information, whether the spreading is extensive or whether the conduct in other respects causes a danger for considerable damage.

An accomplice shall be liable to the same penalty

## **Penal Code § 151 b:**

Any person who by destroying, damaging, or putting out of action any data collection or any installation for supplying power, broadcasting, telecommunication, or transport causes comprehensive disturbance in the public administration or in community life in general shall be liable to imprisonment for a term not exceeding 10 years

Negligent acts of the kind mentioned in the first paragraph shall be punishable by fines or imprisonment for a term not exceeding one year

Accomplices shall be liable to the same penalty



Switzerland

# Unauthorized access to data processing system

## Penal Code:

### Article 143bis: Unauthorized access to data processing system

Anyone, who without authorization, and without the intent of procuring an unlawful gain, accesses a data processing system which are specially protected against unauthorized access, by electronic devices, shall be sentenced to imprisonment or fines

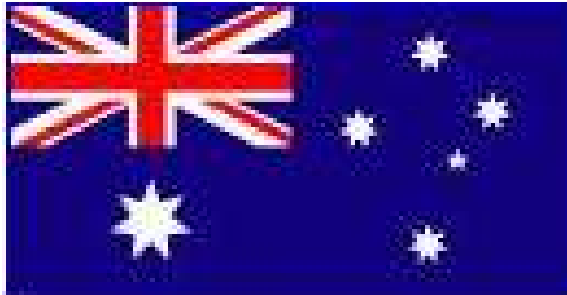
### Article 144bis: Damage to data

1. Anyone, who without authorization alters, erases, or renders useless data which is stored or transferred by electronic or similar means, shall be punished by imprisonment for a term of up to three years or a fine of up to forty thousand Swiss francs if a complaint is made

If the offender has caused serious damage, a sentence of five years penal servitude can be imposed. The offence shall be prosecuted ex officio

2. Any person who produces, imports, circulates, promotes, offers or otherwise makes available programs, which he/ she knows, or ought to assume, are to be used for purposes of committing an offence mentioned in paragraph 1 above, or gives instructions for the production of such programs, shall be punished by imprisonment for a term of up to three years or a fine of up to forty thousand Swiss francs

If the offender commits the offence on a habitual basis for profit, a sentence of up to five years penal servitude can be imposed



# Australia



This site provides the information about Australian Facts & Figures, Government & Parliament, Information & Communications, Law & Justice, Economics, Finance & Tax and other activities

In case of Law & Justice, Australian Law Online provides access to law and justice related information and services from all levels of government. It provides Australians with ready access to clear, understandable, user-friendly information about the Australian legal system and the government organizations that are part of the Australian legal system.



The screenshot shows the homepage of the Australian Government website. At the top, there is a navigation bar with links for 'About', 'Contact', and 'Help'. Below this is the 'australia.gov.au' logo and the text 'Australian Government'. A secondary navigation bar contains links for 'Home', 'Info For', 'Subjects', 'Services', 'About Australia', 'Directories', 'Publications', and 'News & Media'. A search bar is located below the navigation, with a 'Go' button and a link to 'Advanced Search'. The main content area is divided into several sections: 'Government Quicklinks' (listing Parliament of Australia, Prime Minister, Australian Tax Office, business.gov.au, Centrelink, JobSearch, Government Jobs, Departments & Agencies, and State & Territory Websites), 'Information For' (listing Australians Travelling, Jobseekers, Migrants, Students, and Tourists), 'Browse Subjects' (a grid of 18 categories including Australian Facts & Figures, Benefits, Payments & Services, Business & Industry, Culture, History & Sport, Defence & International Relations, Economics, Finance & Tax, Education & Training, Employment & Workplace, Environment & Natural Resources, Family, Home & Community, Government & Parliament, Health & Safety, Immigration, Information & Communications, Law & Justice, Primary Industry, Science & Technology, Tourism & Travel, and Transport), and 'Government Initiatives' (featuring 'Protect Yourself in Five Ways from Skin Cancer', 'Smartraveller', 'National Security', and 'Quarantine Matters!'). A 'SEE MORE SUBJECTS »' link is located at the bottom right of the 'Browse Subjects' section.

## ID theft brings tech to law

Karen Dearne | September 18, 2007

Font Size:   Print Page: 

**POLICY makers will have to abandon their technology-neutral approach to privacy laws in order to tackle the epidemic of identity theft, a leading technology industry body warns.**

"To date, ministers and bureaucrats have avoided getting into the risky area of picking winners in technology," said Stephen Wilson, chair of the Australian Electrical and Electronic Manufacturer's Association (AEE/MA) information security forum.

"This is why we've traditionally had a light-touch regime, but the things we're grappling with now around privacy, identity theft and cybercrime are so difficult we're going to have to take a greater interest in technology.

"That means someone needs to be acknowledging the strengths and weaknesses of different and competing technologies. We're seeing a change of climate around that." The concept of technology neutrality - which meant legislation was drafted to apply to the handling of information in any context - was past its use-by date, Mr Wilson said.

"It's a good legal philosophy, but when it comes down to codes of practice and standards for government and banking services, indifference to the technology at the coalface is really dangerous," he said. Mr Wilson said AEE/MA would welcome a "real debate" on the technological implications for privacy and cybercrime as part of the [Australian Law Reform Commission's preparation of final recommendations on reform of the federal Privacy Act.](#)

Source: <http://www.australianit.news.com.au/>

# The Cybercrime Act 2001

The Cybercrime Act 2001 amended the Criminal Code Act 1995 to replace existing outdated computer offences

478.1 Unauthorized access to, or modification of, restricted data

(1) A person is guilty of an offence if:

- (a) the person causes any unauthorized access to, or modification of, restricted data; and
- (b) the person intends to cause the access or modification; and
- (c) the person knows that the access or modification is unauthorized; and
- (d) one or more of the following applies:
  - (i) the restricted data is held in a Commonwealth computer;
  - (ii) the restricted data is held on behalf of the Commonwealth;
  - (iii) the access to, or modification of, the restricted data is caused by means of a telecommunications service

Penalty: 2 years imprisonment

(2) Absolute liability applies to paragraph (1)(d)

(3) In this section: restricted data means data

(a) held in a computer; and

(b) to which access is restricted by an access control system associated with a function of the computer





India

Legal Service India is the premier and leading Indian Legal portal focused on law and government. It provides access to an extensive and fast-growing online library of free legal resources for use by legal professionals, students, consumers and businesses.

**MINISTRY OF LAW & JUSTICE**

Indian Courts | Causelists | Case Status | Court Websites | Daily Orders | India Code | Judgments | Subordinate Legislation

**Welcome to Ministry of Law & Justice**

Ministry of Law and Justice is the oldest limb of the Government of India dating back to 1833 when the Charter Act 1833 enacted by the British Parliament. The said Act vested for the first time legislative power in a single authority, namely the Governor General in Council. By virtue of this authority and the authority vested under him under section 22 of the Indian Councils Act 1861 the Governor General in Council enacted laws for the country from 1834 to 1920. After the commencement of the Government of India Act 1919 the legislative power was exercised by the Indian Legislature constituted thereunder. The Government of India Act 1919 was followed by the Government of India Act 1935.

[More >>](#)

[About us](#)  
[Honourable Minister's Office](#)  
[Department of Legal Affairs](#)  
[Legislative Department](#)  
[Law Commission of India](#)  
[Department of Justice](#)  
[Official lang. Wing\(Hindi\)](#)  
[NCRWC](#)  
[On-line databases](#)

[Contact Us](#)

The national portal of India  
**india.gov.in**

Site Last Updated on:  
**01 January, 2008**

- [Principal Accounts Office](#)
- [Sanctions in respect of Grants-in-aid / Loans to State Governments](#)
- [Tenders \*\*NEW\*\*](#)
- [List of Notaries Appointed \(as on October, 2007\)](#)
- [Application Form for Notary Public](#)

## The Indian Information Technology Act and Spamming

Author: [Rahul Goel](#), A Sense Of Place Network | February 8th, 2006

Communities: [Digital Divide in INDIA](#)

Today, the technology is the driving force of any economy. However, to check that such driving force follows the path of law and works in larger interest of the society, all countries need a robust legislation. Internet is one such technology, which spans across the globe, out of direct control of any single country or legislation. The countries like United States and United Kingdom have enacted legislations to safeguard the interests of their citizens and traders. India enacted its first legislation, the Information Technology Act, 2000 to regulate Internet and e-commerce in 2000. However, as technology evolved, the offences in this area took a different path and the provisions of the existing legislation were found to be ineffective in curbing such crimes.

A couple of isolated cases of theft relating to confidential data of the client from BPOs/ call centers rocked the entire information technology sector in India. It was soon realized that the existing Act needs to be amended to include provisions relating to misuse of evolved technology. The Government of India with an aim to amend the Information technology Act, 2000 constituted an Expert Committee. The Committee after reviewing several issues including issues relating to privacy and protection of data has recently submitted its recommendations and suggestions to the Government of India.

The Committee has tried to address issues relating to electronic contracts, breach of confidentiality and privacy, child pornography, electronic/ digital signatures etc. However, the recommendations are silent on prosecution as regard to phishing, pharming and spamming.



Source: <http://www.digitaldivide.net/>



## THE INFORMATION TECHNOLOGY ACT, 2000 (No. 21 of 2000)

### CHAPTER XI

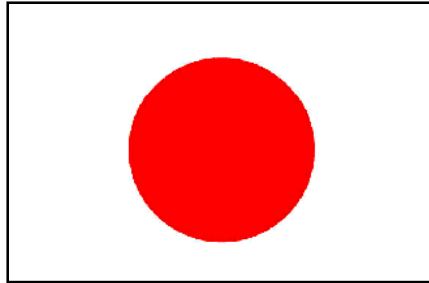
### OFFENCES

#### 66. Hacking with computer system

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both





Japan

This site mentions not only mentions the basic rules (basic legislation) applicable in daily life but also the basic judicial framework under which these rules are faithfully observed.

**The Ministry of Justice**

**Information**

- Public Announcement on the competition for "Linguistic Advisory Services (English)"
- The Information Desk for Direct Investment to Japan
- Gaikokuho-Jimu-Bengoshi ("Gaiben", Registered Foreign Lawyers)
- Nationality Administration
- The Electronic Commerce
- Law relating to recognition and assistance for foreign insolvency proceedings
- Japanese Corporate Law: Drastic Changes In 2000-2001 & The Future

PREFACE

Topics

- New Immigration Procedures(2011/2007)

Historical Background

Minister, Senior Vice-Minister, Parliamentary Secretary

Organization

## Boy hacker arrested over violation of computer law.

Source: 🇵🇭 Asia Africa Intelligence Wire

Publication Date: 01-NOV-03

(From The Yomiuri Shimbun/Daily Yomiuri)

Boy hacker arrested over violation of computer law

Yomiuri

Police have arrested a 17-year-old Brazilian boy living in Tochigi Prefecture on suspicion of violating the Unauthorized Computer Access Law, the police said Friday.

The boy is a member of an international group of hackers responsible for hacking into more than 1,000 Web sites in 33 countries.

The Metropolitan Police Department arrested the boy on suspicion of violating the Unauthorized Computer Access Law.

He reportedly has told investigators from the MPD's center overseeing high-tech-related crimes that he thought major companies would want to employ him if he displayed his hacking skills.

The boy used his personal computer to illegally access the computer system of Kyoto University Hospital on July 10. He left phrases written in English including "s3r14l k1l13r was here" on the Web site of the university's Human Brain Research Center.

According to the police, the boy went by the nickname "s3r14l k1l13r"--which can be read as "serial killer"--in the group.

The boy also is suspected of hacking into and defacing the Web sites of a private high school and a computer servicing company in the metropolitan area.

The boy was a member of an international group of hackers who named themselves "CyberLords." The group was formed near the end of last year by eight hackers, including Americans and Brazilians, who became acquainted through a Web site used exclusively by hackers.

Group members exchanged information with each other about software programs designed to attack computer systems and security flaws in Web sites that could be exploited, and randomly attacked Web sites all over the world, the police said.

The hackers vied with each other to hack into Web sites and published on the Internet their hacking "track record."

Source: <http://www.accessmylibrary.com/>

Copyright © by **EC-Council**

All Rights Reserved. Reproduction is Strictly Prohibited

Law No. 128 of 1999 (in effect from February 3, 2000)

Husei access kinski hou

Article 3. No person shall conduct an act of unauthorized computer access.

(1) An act of making available a specific use which is restricted by an access control function by making in operation a specific computer having that access control function through inputting into that specific computer, via telecommunication line, another person's identification code for that access control function

(2) An act of making available a restricted specific use by making in operation a specific computer having that access control function through inputting into it, via telecommunication line, any information (excluding an identification code) or command that can evade the restrictions placed by that access control function on that specific use

Source: <http://www.mosstingrett.no/>

(3) An act of making available a restricted specific use by making in operation a specific computer, whose specific use is restricted by an access control function installed into another specific computer which is connected, via a telecommunication line, to that specific computer, through inputting into it, via a telecommunication, any information or command that can evade the restriction concerned

Article 4. No person shall provide another person's identification code relating to an access control function to a person other than the access administrator for that access control function or the authorized user for that identification code, in indicating that it is the identification code for which specific computer's specific use, or at the request of a person who has such knowledge, excepting the case where such acts are conducted by that access administrator, or with the approval of that access administrator or of that authorized user

Article 8. A person who falls under one of the following items shall be punished with penal servitude for not more than one year or a fine of not more than 500,000 yen:

(1) A person who has infringed the provision of Article 3, paragraph 1;

Article 9. A person who has infringed the provision of Article 4 shall be punished with a fine of not more than 300,000 yen





Singapore



SINGOV, is the default homepage for the Singapore Government Online. The above site directs you to SIGNOV site. SINGOV is the "Government" component of the Singapore Government Online. It serves as a convenient launch pad for users to locate information on the Singapore Government - such as government news and policies, leadership and bureacracy, official statistics put out by the government, as well as details and contact information of public service agencies

The screenshot shows the Singapore Government website's 'SINGOV' section. At the top right is the Singapore Government logo with the tagline 'Integrity • Service • Excellence'. Below it are navigation tabs for 'GOVERNMENT', 'CITIZENS & RESIDENTS', 'BUSINESSES', and 'NON-RESIDENTS'. The main header features the 'SINGOV Government Information' logo, a search bar with a 'Go' button, and a dropdown menu set to 'Within All Government Websites'. A secondary navigation bar includes links for 'Home', 'About Us', 'Careers', 'Useful Links', 'Rate Our Website', and 'A-Z Government List'. The main content area is titled 'Information & Policies' and lists various legal topics: Law, Alternative Dispute Resolution, Constituencies Boundaries, Dispute Resolution, How Laws are Made in Singapore, Insol Search, Insolvencies, Intellectual Property Rights, Latest Bills, and Law Resources.



## Singapore "cyberterrorism" laws raise fears of abuse.

Source:  Europe Intelligence Wire

Publication Date: 23-NOV-03

(From Agence France Presse)

New laws allowing Singapore to launch pre-emptive strikes against computer hackers have raised fears that Internet controls are being tightened and privacy compromised in the name of fighting terrorism.

The city-state's parliament has approved tough new legislation aimed at stopping "cyberterrorism," referring to computer crimes that are endanger national security, foreign relations, banking and essential public services.

Security agencies can now patrol the Internet and swoop down on hackers suspected of plotting to use computer keyboards as weapons of mass disruption.

Violators of the Computer Misuse Act such as website hackers can be jailed up to three years or fined up to 10,000 Singapore dollars (5,800 US).

But a vocal opposition fear the law will be abused.

"It could be misused to invade into the privacy of citizens to gather information," said Sinapan Samydorai, president of Think Centre, a civil liberties group. He said the new laws could be used as an "instrument of oppression" by the government.

An online poll by popular Internet portal Yahoo Singapore showed that 70 percent of respondents felt the new laws gave the authorities too much power, and they were afraid they were being watched.

But the Ministry of Home Affairs told AFP that "any measures to be deployed will be non-intrusive in nature."

"For example, any scanning programme deployed will not intrude into a subscriber's personal computer. It will only scan the Internet passively to determine vulnerabilities in the affected network," a spokeswoman said.

Any private information about "law-abiding citizens" security agencies may come across in their hunt for hackers will be protected, she added.

The new measures have been likened by critics to the Internal Security Act, which has been used to detain political dissidents and radicals without trial.

Source: <http://www.accessmylibrary.com/>

Copyright © by **EC-Council**

## Chapter 50A: Computer misuse Act

Section 3 – (1) Any person who knowingly causes a computer to perform any function for the purpose of securing access without authority, shall be liable on conviction to a fine not exceeding \$ 5.000 or to imprisonment for a term not exceeding 2 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding \$ 50.000 or to imprisonment for a term not exceeding 7 years or to both

### Section 4: Access with intent to commit or facilitate commission of offence

(1) This section shall apply to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years.

(2) Any person guilty of an offence under this section shall be liable on conviction to a not exceeding \$ 50.000 or to imprisonment for a term not exceeding 10 years or to both



Korea

## S KOREA TO IMPOSE 3-YR PRISON TERM FOR CONVICTED HACKERS.

Source: 🇰🇷 AsiaPulse News

Publication Date: 01-AUG-03

SEOUL, Aug 1 Asia Pulse - Those convicted of attempting hacking will face punishment of up to three years or 30 million won (US\$25,410) in fines from next year, the Ministry of Information and Communications said Friday.

The current communication law mandates punishment only when hacking has been carried out.

To that end, the ministry said, it has already mapped out an amendment to strengthen regulations on information protection and ban on personal information leakage.

The draft contains a new regulation that punishes hackers trying to access to others' networks without permission or in excess of the scope of their permission, the ministry said.

It also would enable information service providers to temporarily suspend service to certain clients whose security measures, such as computer vaccines, are deemed insufficient, according to the ministry.

The draft will be referred to the National Assembly in September after reviews by other ministries, with an amended law likely to be implemented in March, it added.

(Yonhap) 01-08 1219

Source: <http://www.accessmylibrary.com/>

## CHAPTER VI Stability of the Information and Communications Network

### Article 48 (Prohibition on Act of Infiltrating into Information and Communications Networks, etc.)

(1) Any person shall be prohibited from infiltrating into information and communications networks without any justifiable access right or beyond his/her permitted access right

(2) Any person shall be prohibited from transmitting or distributing any program (hereinafter referred to as a "malicious program") that may damage, disrupt, and destroy the information and communications system, alter and forge the data or programs, etc., or hinder the operation thereof without any justifiable reasons

(3) Any person shall be prohibited from sending a large volume of signals or data for the purpose of hindering the stable operation of information and communications networks or from causing troubles in information and communications networks using the method of getting unfair instructions processed

## Article 49 (Protection of Secrets, etc.)

Any person shall be prohibited from damaging the information of other persons or from infringing, stealing or leaking the secrets of other persons, which are processed, stored or transmitted by information and communications networks

## CHAPTER IX PENAL PROVISIONS

### Article 61 (Penal Provisions)

(1) Any person who has defamed any other person by alleging openly facts through information and communications network with the purpose of slandering him/her shall be punished by imprisonment with or without prison labor for not more than 3 years or by a fine not exceeding 20 million won

(2) Any person who has defamed any other person by alleging openly false facts through information and communications network with the purpose of slandering him/her shall be punished by imprisonment with prison labor for not more than 7 years or the suspension of disqualification for not more than 10 years, or by a fine not exceeding 50 million won



# Malaysia



Laws in Malaysia has refined and strengthened its legal system to ensure that citizens are protected in a fair manner. Those laws are mentioned in the following website



### Three new cyber laws to be introduced this year.

Source: 📰 Asia Africa Intelligence Wire

Publication Date: 30-JAN-04

(From Business Times (Malaysia))

THREE new cyber laws to beef up rules and regulations governing the use of information and communications technology (ICT) are expected to be approved by Parliament this year.

The proposed laws are the Electronic Government Act, the Electronic Transactions Act and the Personal Data Protection Act.

Energy, Communications and Multimedia Ministry secretary-general Datuk Dr Halim Shafie said the Malaysian Administrative Modernisation and Management Planning Unit is finalising the draft of the Electronic Government Act, and will submit it to the Government for approval.

Addressing participants of the ICT and Venture Capital Financing Forum 2004 in Kuala Lumpur yesterday, he said the other two drafts have been submitted to the Attorney-General's Chamber.

Since 1997, cyber laws passed by Parliament include the Digital Signature Act 1997, the Computer Crimes Act 1997, the Copyright (Amendment) Act 1997, the Telemedicine Act 1997, and the Communications and Multimedia Act 1998.

Meanwhile, National Economic Action Council (NEAC) executive director Datuk Mustapa Mohamed said Malaysia has made great strides in the development of ICT, particularly with the Multimedia Super Corridor (MSC).

As at January 13 2004, he said, there were 976 MSC-status companies, comprising 934 MSC technology companies, 33 institutions of higher learning with MSC status, and nine incubator companies.

"Many of these achievements have far surpassed initial targets," Mustapa said.

He also said there are now 2,700 ICT companies operating in Malaysia, covering hardware manufacturing, software development, computer retailing, ICT consultancy and other ICT services.

To enhance the development of the ICT industry in Malaysia, he said, the National Information Technology Council was formed to steer Malaysia towards the knowledge empowerment of Vision 2020, strongly believing information and knowledge can serve as the country's most valuable assets in this current millennium.

Mustapa's keynote address was read out by NEAC adviser Datuk Rahmah Abu Kassim.

On the venture capital industry, Mustapa said the industry can play a critical role in enabling Malaysia to shift successfully from a capital-intensive economy to an advanced and globally competitive knowledge economy.

Source: <http://www.accessmylibrary.com/>

## COMPUTER CRIMES ACT 1997

### PART II OFFENCES

3 (1) A person shall be guilty of an offence if

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

a. the access he intends to secure is unauthorized; and

(c) he knows at the time when he causes the computer to perform the function that that is the case

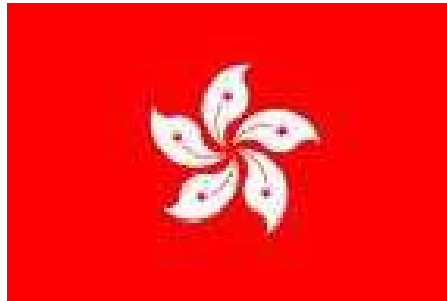
(2) The intent a person has to have to commit an offence under this section need not be directed at -

(a) any particular program or data;

(b) a program or data of any particular kind; or

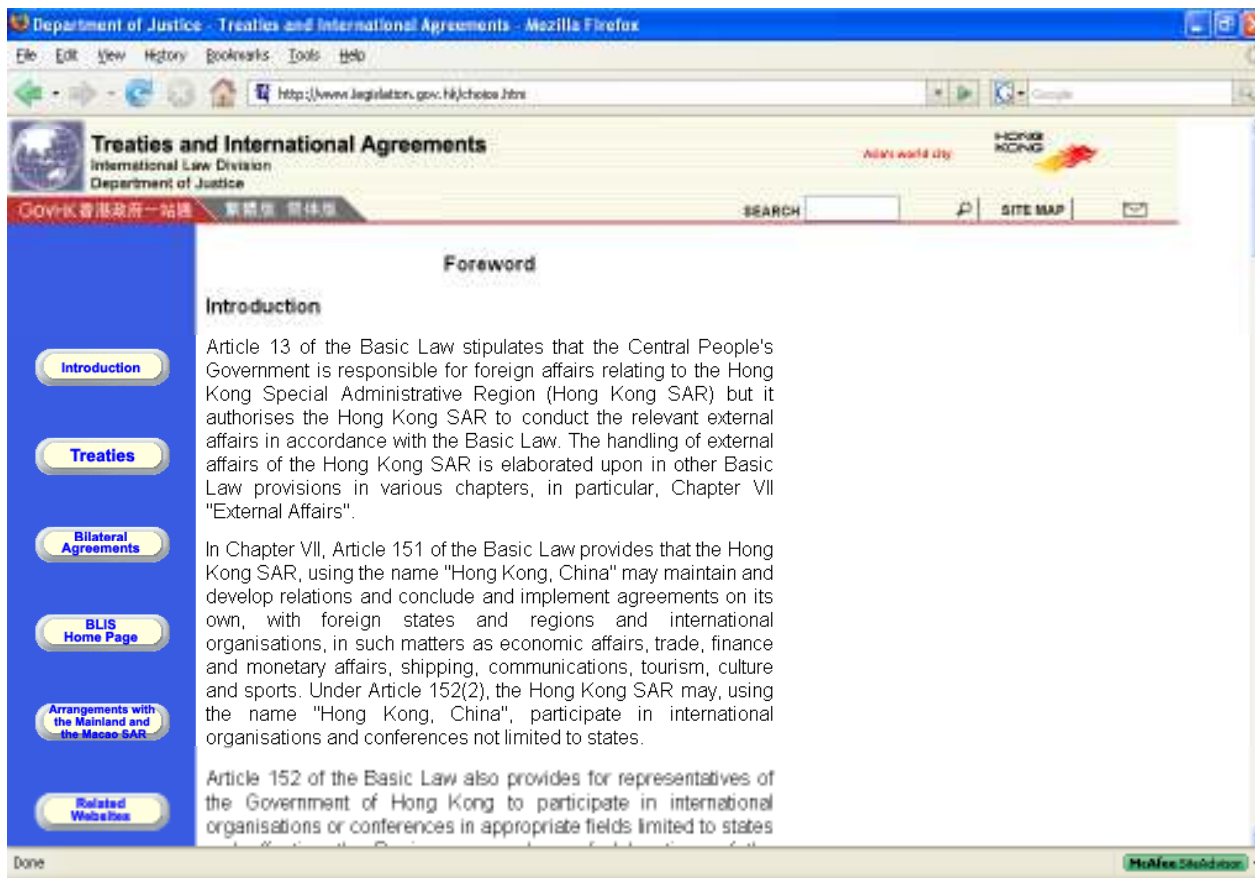
(c) a program or data held in any particular computer

1. A person guilty of an offence under this section shall on conviction be liable to a fine not exceeding fifty thousand ringgit or to imprisonment not exceeding five years or to both



Hongkong

Basic Law of Hongkong website specifies that the Central People's Government is not only responsible for foreign affairs but also authorizes the Hong Kong Special Administrative Region to conduct the relevant external affairs in accordance with the law



Boy arrested for hacking into computers

Saturday, 26 January, 2008

A 14-year-old Hong Kong boy has been arrested for hacking into the computers of eight of the territory's secondary schools, a news report said.

The teenage computer whiz hacked into password-sensitive online forums where students and teachers exchange questions and answers, the South China Morning Post reported.

He was arrested after the information technology company that provides computer services to the eight schools called in police after discovering the network had been hacked.

The schoolboy was collared by police in an early-morning raid at his home and his computer was seized for examination by experts, the newspaper said.

After his arrest, the boy told police he had hacked into the network "for fun" after being taught how to do it by a classmate. He is not believed to have stolen any sensitive or secret data.

The schoolboy, who has not been named, could technically face a jail term of up to five years under Hong Kong's strict anti-computer hacking laws. His classmate is also expected to be arrested.

Source: <http://news.sbs.com.au/>

Copyright © by **EC-Council**

All Rights Reserved. Reproduction is Strictly Prohibited

## Unauthorized access to computer by telecommunications

- (1) Any person who, by telecommunications, knowingly causes a computer to perform any function to obtain unauthorized access to any program or data held in a computer commits an offence and is liable on conviction to a fine of \$20000. (Amended 36 of 2000 s. 28)
- (2) For the purposes of subsection (1)-
  - (a) the intent of the person need not be directed at-
    - (i) any particular program or data;
    - (ii) a program or data of a particular kind; or
    - (iii) a program or data held in a particular computer
  - (b) access of any kind by a person to any program or data held in a computer is unauthorized if he is not entitled to control access of the kind in question to the program or data held in the computer and-
    - (i) he has not been authorized to obtain access of the kind in question to the program or data held in the computer by any person who is so entitled;

(ii) he does not believe that he has been so authorized; and

(iii) he does not believe that he would have been so authorized if he had applied for the appropriate authority

(3) Subsection (1) has effect without prejudice to any law relating to powers of inspection, search or seizure.

(4) Notwithstanding section 26 of the Magistrates Ordinance (Cap 227), proceedings for an offence under this section may be brought at any time within 3 years of the commission of the offence or within 6 months of the discovery of the offence by the prosecutor, whichever period expires first





In this module, we have reviewed various laws and acts related to hacking

These hacking laws has covered the laws present in maximum countries including United Status, United Kingdom, Europe, Japan, Australia, India, Germany, Singapore, Belgium, Brazil, Canada, France and Italy