Penal Codes Relevant to Computer Crime in various Countries

United States:

Sec. 33.01. DEFINITIONS. In this chapter:

(1) "Access" means to approach, instruct, communicate with, store data in, retrieve or intercept data from, alter data or computer software in, or otherwise make use of any resource of a computer, computer network, computer program, or computer system.

(2) "Aggregate amount" means the amount of:

(A) any direct or indirect loss incurred by a victim, including the value of money, property, or service stolen or rendered unrecoverable by the offense; or

(B) any expenditure required by the victim to verify that a computer, computer network, computer program, or computer system was not altered, acquired, damaged, deleted, or disrupted by the offense.

(3) "Communications common carrier" means a person who owns or operates a telephone system in this state that includes equipment or facilities for the conveyance, transmission, or reception of communications and who receives compensation from persons who use that system.

(4) "Computer" means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device.

(5) "Computer network" means the interconnection of two or more computers or computer systems by satellite, microwave, line, or other communication medium with the capability to transmit information among the computers.

(6) "Computer program" means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data or perform specific functions.

(7) "Computer services" means the product of the use of a computer, the information stored in the computer, or the personnel supporting the computer, including computer time, data processing, and storage functions.

(8) "Computer system" means any combination of a computer or computer network with the documentation, computer software, or physical facilities supporting the computer or computer network.

(9) "Computer software" means a set of computer programs, procedures, and associated documentation related to the operation of a computer, computer system, or computer network.

(10) "Computer virus" means an unwanted computer program or other set of instructions inserted into a computer's memory, operating system, or program that is specifically constructed with the ability to replicate itself or to affect the other programs or files in the computer by attaching a copy of the unwanted program or other set of instructions to one or more computer programs or files.

(10-a) "Critical infrastructure facility" means:

(A) a chemical manufacturing facility;

(B) a refinery;

(C) an electrical power generating facility, substation, switching station, electrical control center, or electrical transmission or distribution facility;

(D) a water intake structure, water treatment facility, wastewater treatment plant, or pump station;

(E) a natural gas transmission compressor station;

(F) a liquid natural gas terminal or storage facility;

(G) a telecommunications central switching office;

(H) a port, railroad switching yard, trucking terminal, or other freight transportation facility;

(I) a gas processing plant, including a plant used in the processing, treatment, or fractionation of natural gas;

(J) a transmission facility used by a federally licensed radio or television station; or

(K) a cable television or video service provider headend.

(11) "Data" means a representation of information, knowledge, facts, concepts, or instructions that is being prepared or has been prepared in a formalized manner and is intended to be stored or processed, is being stored or processed, or has been stored or processed in a computer. Data may be embodied in any form, including but not limited to computer printouts, magnetic storage media, laser storage media, and punchcards, or may be stored internally in the memory of the computer.

(12) "Effective consent" includes consent by a person legally authorized to act for the owner. Consent is not effective if:

(A) induced by deception, as defined by Section 31.01, or induced by coercion;

(B) given by a person the actor knows is not legally authorized to act for the owner;

(C) given by a person who by reason of youth, mental disease or defect, or intoxication is known by the actor to be unable to make reasonable property dispositions;

(D) given solely to detect the commission of an offense; or

(E) used for a purpose other than that for which the consent was given.

(13) "Electric utility" has the meaning assigned by Section 31.002, Utilities Code.

(14) "Harm" includes partial or total alteration, damage, or erasure of stored data, interruption of computer services, introduction of a computer virus, or any other loss, disadvantage, or injury that might reasonably be suffered as a result of the actor's conduct.

(14-a) "Identifying information" has the meaning assigned by Section 32.51.

(15) "Owner" means a person who:

(A) has title to the property, possession of the property, whether lawful or not, or a greater right to possession of the property than the actor;

(B) has the right to restrict access to the property; or

(C) is the licensee of data or computer software.

(16) "Property" means:

(A) tangible or intangible personal property including a computer, computer system, computer network, computer software, or data; or

(B) the use of a computer, computer system, computer network, computer software, or data.

Added by Acts 1985, 69th Leg., ch. 600, Sec. 1, eff. Sept. 1, 1985. Amended by Acts 1989, 71st Leg., ch. 306, Sec. 1, eff. Sept. 1, 1989; Acts 1993, 73rd Leg., ch. 900, Sec. 1.01, eff. Sept. 1, 1994; Acts 1997, 75th Leg., ch. 306, Sec. 1, eff. Sept. 1, 1997; Acts 1999, 76th Leg., ch. 62, Sec. 18.44, eff. Sept. 1, 1999.

Amended by:

Acts 2011, 82nd Leg., R.S., Ch. 1044, Sec. 1, eff. September 1, 2011.

Sec. 33.02. BREACH OF COMPUTER SECURITY. (a) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

(b) An offense under Subsection (a) is a Class B misdemeanor, except that the offense is a state jail felony if:

(1) the defendant has been previously convicted two or more times of an offense under this chapter; or

(2) the computer, computer network, or computer system is owned by the government or a critical infrastructure facility.

(b-1) A person commits an offense if with the intent to defraud or harm another or alter, damage, or delete property, the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

(b-2) An offense under Subsection (b-1) is:

(1) a state jail felony if the aggregate amount involved is less than $20,000;

(2) a felony of the third degree if the aggregate amount involved is $20,000 or more but less than $100,000;

(3) a felony of the second degree if:

(A) the aggregate amount involved is $100,000 or more but less than $200,000;

(B) the aggregate amount involved is any amount less than $200,000 and the computer, computer network, or computer system is owned by the government or a critical infrastructure facility; or

(C) the actor obtains the identifying information of another by accessing only one computer, computer network, or computer system; or

(4) a felony of the first degree if:

(A) the aggregate amount involved is $200,000 or more; or

(B) the actor obtains the identifying information of another by accessing more than one computer, computer network, or computer system.

(c) When benefits are obtained, a victim is defrauded or harmed, or property is altered, damaged, or deleted in violation of this section, whether or not in a single incident, the conduct may be considered as one offense and the value of the benefits obtained and of the losses incurred because of the fraud, harm, or alteration, damage, or deletion of property may be aggregated in determining the grade of the offense.

(d) A person who is subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.

(e) It is a defense to prosecution under this section that the person acted with the intent to facilitate a lawful seizure or search of, or lawful access to, a computer, computer network, or computer system for a legitimate law enforcement purpose.

Added by Acts 1985, 69th Leg., ch. 600, Sec. 1, eff. Sept. 1, 1985. Amended by Acts 1989, 71st Leg., ch. 306, Sec. 2, eff. Sept. 1, 1989; Acts 1993, 73rd Leg., ch. 900, Sec. 1.01, eff. Sept. 1, 1994; Acts 1997, 75th Leg., ch. 306, Sec. 2, eff. Sept. 1, 1997; Acts 2001, 77th Leg., ch. 1411, Sec. 1, eff. Sept. 1, 2001.

Amended by:

Acts 2011, 82nd Leg., R.S., Ch. 1044, Sec. 2, eff. September 1, 2011.

Sec. 33.021. ONLINE SOLICITATION OF A MINOR. (a) In this section:

(1) "Minor" means:

(A) an individual who represents himself or herself to be younger than 17 years of age; or

(B) an individual whom the actor believes to be younger than 17 years of age.

(2) "Sexual contact," "sexual intercourse," and "deviate sexual intercourse" have the meanings assigned by Section 21.01.

(3) "Sexually explicit" means any communication, language, or material, including a photographic or video image, that relates to or describes sexual conduct, as defined by Section 43.25.

(b) A person who is 17 years of age or older commits an offense if, with the intent to arouse or gratify the sexual desire of any person, the person, over the Internet, by electronic mail or text message or other electronic message service or system, or through a commercial online service, intentionally:

(1) communicates in a sexually explicit manner with a minor; or

(2) distributes sexually explicit material to a minor.

(c) A person commits an offense if the person, over the Internet, by electronic mail or text message or other electronic message service or system, or through a commercial online service, knowingly solicits a minor to meet another person, including the actor, with the intent that the minor will engage in sexual contact, sexual intercourse, or deviate sexual intercourse with the actor or another person.

(d) It is not a defense to prosecution under Subsection (c) that:

(1) the meeting did not occur;

(2) the actor did not intend for the meeting to occur; or

(3) the actor was engaged in a fantasy at the time of commission of the offense.

(e) It is a defense to prosecution under this section that at the time conduct described by Subsection (b) or (c) was committed:

(1) the actor was married to the minor; or

(2) the actor was not more than three years older than the minor and the minor consented to the conduct.

(f) An offense under Subsection (b) is a felony of the third degree, except that the offense is a felony of the second degree if the minor is younger than 14 years of age or is an individual whom the actor believes to be younger than 14 years of age at the time of the commission of the offense. An offense under Subsection (c) is a felony of the second degree.

(g) If conduct that constitutes an offense under this section also constitutes an offense under any other law, the actor may be prosecuted under this section, the other law, or both.

Added by Acts 2005, 79th Leg., Ch. 1273, Sec. 1, eff. June 18, 2005.
Amended by:
Acts 2007, 80th Leg., R.S., Ch. 610, Sec. 2, eff. September 1, 2007.
Acts 2007, 80th Leg., R.S., Ch. 1291, Sec. 7, eff. September 1, 2007.

Sec. 33.03. DEFENSES. It is an affirmative defense to prosecution under Section 33.02 that the actor was an officer, employee, or agent of a communications common carrier or electric utility and committed the proscribed act or acts in the course of employment while engaged in an activity that is a necessary incident to the rendition of service or to the protection of the rights or property of the communications common carrier or electric utility.

Added by Acts 1985, 69th Leg., ch. 600, Sec. 1, eff. Sept. 1, 1985. Renumbered from Penal Code Sec. 33.04 and amended by Acts 1993, 73rd Leg., ch. 900, Sec. 1.01, eff. Sept. 1, 1994.

Sec. 33.04. ASSISTANCE BY ATTORNEY GENERAL. The attorney general, if requested to do so by a prosecuting attorney, may assist the prosecuting attorney in the investigation or prosecution of an offense under this chapter or of any other offense involving the use of a computer.

Added by Acts 1985, 69th Leg., ch. 600, Sec. 1, eff. Sept. 1, 1985. Renumbered from Penal Code Sec. 33.05 by Acts 1993, 73rd Leg., ch. 900, Sec. 1.01, eff. Sept. 1, 1994.

Sec. 33.05. TAMPERING WITH DIRECT RECORDING ELECTRONIC VOTING MACHINE. (a) In this section:

(1) "Direct recording electronic voting machine" has the meaning assigned by Section 121.003, Election Code.

(2) "Measure" has the meaning assigned by Section 1.005, Election Code.

(b) A person commits an offense if the person knowingly accesses a computer, computer network, computer program, computer software, or computer system that is a part of a voting system that uses direct recording electronic voting machines and by means of that access:

(1) prevents a person from lawfully casting a vote;

(2) changes a lawfully cast vote;

(3) prevents a lawfully cast vote from being counted; or

(4) causes a vote that was not lawfully cast to be counted.

(c) An offense under this section does not require that the votes as affected by the person's actions described by Subsection (b) actually be the votes used in the official determination of the outcome of the election.

(d) An offense under this section is a felony of the first degree.

(e) Notwithstanding Section 15.01(d), an offense under Section 15.01(a) is a felony of the third degree if the offense the actor intends to commit is an offense under this section.

(f) With the consent of the appropriate local county or district attorney, the attorney general has concurrent jurisdiction with that consenting local prosecutor to investigate or prosecute an offense under this section.

Added by Acts 2005, 79th Leg., Ch. 470, Sec. 1, eff. September 1, 2005.
Amended by:
Acts 2009, 81st Leg., R.S., Ch. 503, Sec. 1, eff. September 1, 2009.

Sec. 33.07. ONLINE IMPERSONATION. (a) A person commits an offense if the person, without obtaining the other person's consent and with the intent to harm, defraud, intimidate, or threaten any person, uses the name or persona of another person to:

(1) create a web page on a commercial social networking site or other Internet website; or

(2) post or send one or more messages on or through a commercial social networking site or other Internet website, other than on or through an electronic mail program or message board program.

(b) A person commits an offense if the person sends an electronic mail, instant message, text message, or similar communication that references a name, domain address, phone number, or other item of identifying information belonging to any person:

(1) without obtaining the other person's consent;

(2) with the intent to cause a recipient of the communication to reasonably believe that the other person authorized or transmitted the communication; and

(3) with the intent to harm or defraud any person.

(c) An offense under Subsection (a) is a felony of the third degree. An offense under Subsection (b) is a Class A misdemeanor, except that the offense is a felony of the third degree if the actor commits the offense with the intent to solicit a response by emergency personnel.

(d) If conduct that constitutes an offense under this section also constitutes an offense under any other law, the actor may be prosecuted under this section, the other law, or both.

(e) It is a defense to prosecution under this section that the actor is any of the following entities or that the actor's conduct consisted solely of action taken as an employee of any of the following entities:

(1) a commercial social networking site;

(2) an Internet service provider;

(3) an interactive computer service, as defined by 47 U.S.C. Section 230;

(4) a telecommunications provider, as defined by Section 51.002, Utilities Code; or

(5) a video service provider or cable service provider, as defined by Section 66.002, Utilities Code.

(f) In this section:

(1) "Commercial social networking site" means any business, organization, or other similar entity operating a website that permits persons to become registered users for the purpose of establishing personal relationships with other users through direct or real-time communication with other users or the creation of web pages or profiles available to the public or to other users. The term does not include an electronic mail program or a message board program.

(2) "Identifying information" has the meaning assigned by Section 32.51.

Added by Acts 2009, 81st Leg., R.S., Ch. 911, Sec. 1, eff. September 1, 2009.
Amended by:
Acts 2011, 82nd Leg., R.S., Ch. 282, Sec. 1, eff. September 1, 2011.
Acts 2011, 82nd Leg., R.S., Ch. 282, Sec. 2, eff. September 1, 2011.

Australia:

Division 476—Preliminary
476.1 Definitions

(1) In this Part:

access to data held in a computer means:

(a) the display of the data by the computer or any other output of the data from the computer; or

(b) the copying or moving of the data to any other place in the computer or to a data storage device; or

(c) in the case of a program—the execution of the program.

Commonwealth computer means a computer owned, leased or operated by a Commonwealth entity.

data includes:

(a) information in any form; or

(b) any program (or part of a program).

data held in a computer includes:

(a) data held in any removable data storage device for the time being held in a computer; or

(b) data held in a data storage device on a computer network of which the computer forms a part.

data storage device means a thing (for example, a disk or file server) containing, or designed to contain, data for use by a computer.

electronic communication means a communication of information in any form by means of guided or unguided electromagnetic energy.

impairment of electronic communication to or from a computer includes:

(a) the prevention of any such communication; or

(b) the impairment of any such communication on an electronic link or network used by the computer;

but does not include a mere interception of any such communication.

modification, in respect of data held in a computer, means:

(a) the alteration or removal of the data; or

(b) an addition to the data.

telecommunications service means a service for carrying communications by means of guided or unguided electromagnetic energy or both.

unauthorised access, modification or impairment has the meaning given in section 476.2.

(2) In this Part, a reference to:

(a) access to data held in a computer; or

(b) modification of data held in a computer; or

(c) the impairment of electronic communication to or from a computer;

is limited to such access, modification or impairment caused, whether directly or indirectly, by the execution of a function of a computer.

476.2 Meaning of *unauthorised access, modification or impairment*

(1) In this Part:

(a) access to data held in a computer; or

(b) modification of data held in a computer; or

(c) the impairment of electronic communication to or from a computer; or

(d) the impairment of the reliability, security or operation of any data held on a computer disk, credit card or other device used to store data by electronic means;

by a person is unauthorised if the person is not entitled to cause that access, modification or impairment.

(2) Any such access, modification or impairment caused by the person is not unauthorised merely because he or she has an ulterior purpose for causing it.

(3) For the purposes of an offence under this Part, a person causes any such unauthorised access, modification or impairment if the person's conduct substantially contributes to it.

(4) For the purposes of subsection (1), if:

(a) a person causes any access, modification or impairment of a kind mentioned in that subsection; and

(b) the person does so under a warrant issued under the law of the Commonwealth, a State or a Territory;

the person is entitled to cause that access, modification or impairment.

476.3 Geographical jurisdiction

Section 15.1 (extended geographical jurisdiction—Category A) applies to offences under this Part.

476.4 Saving of other laws

(1) This Part is not intended to exclude or limit the operation of any other law of the Commonwealth, a State or a Territory.

(2) Subsection (1) has effect subject to section 476.5.

476.5 Liability for certain acts

(1) A staff member or agent of ASIS or DSD (the ***agency***) is not subject to any civil or criminal liability for any computer-related act done outside Australia if the act is done in the proper performance of a function of the agency.

(2) A person is not subject to any civil or criminal liability for any act done inside Australia if:

(a) the act is preparatory to, in support of, or otherwise directly connected with, overseas activities of the agency concerned; and

(b) the act:

(i) taken together with a computer-related act, event, circumstance or result that took place, or was intended to take place, outside Australia, could amount to an offence; but

(ii) in the absence of that computer-related act, event, circumstance or result, would not amount to an offence; and

(c) the act is done in the proper performance of a function of the agency.

(2A) Subsection (2) is not intended to permit any act in relation to premises, persons, computers, things, or telecommunications services in Australia, being:

(a) an act that ASIO could not do without a Minister authorising it by warrant issued under Division 2 of Part III of the *Australian Security Intelligence Organisation Act 1979* or under Part III of the *Telecommunications (Interception) Act 1979*; or

(b) an act to obtain information that ASIO could not obtain other than in accordance with section 283 of the *Telecommunications Act 1997*.

(2B) The Inspector-General of Intelligence and Security may give a certificate in writing certifying any fact relevant to the question of whether an act was done in the proper performance of a function of an agency.

(2C) In any proceedings, a certificate given under subsection (2B) is prima facie evidence of the facts certified.

(3) In this section:

ASIS means the Australian Secret Intelligence Service.

civil or criminal liability means any civil or criminal liability (whether under this Part, under another law or otherwise).

computer-related act, event, circumstance or result means an act, event, circumstance or result involving:

(a) the reliability, security or operation of a computer; or

(b) access to, or modification of, data held in a computer or on a data storage device; or

(c) electronic communication to or from a computer; or

(d) the reliability, security or operation of any data held in or on a computer, computer disk, credit card, or other data storage device; or

(e) possession or control of data held in a computer or on a data storage device; or

(f) producing, supplying or obtaining data held in a computer or on a data storage device.

DSD means that part of the Department of Defence known as the Defence Signals Directorate.

staff member means:

(a) in relation to ASIS—the Director-General of ASIS or a member of the staff of ASIS (whether an employee of ASIS, a consultant to ASIS, or a person who is made available by another Commonwealth or State authority or other person to perform services for ASIS); and

(b) in relation to DSD—the Director of DSD or a member of the staff of DSD (whether an employee of DSD, a consultant to DSD, or a person who is made available by another Commonwealth or State authority or other person to perform services for DSD).

Division 477—Serious computer offences

477.1 Unauthorised access, modification or impairment with intent to commit a serious offence

Intention to commit a serious Commonwealth, State or Territory offence

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

(a) the person causes:

(i) any unauthorised access to data held in a computer; or

(ii) any unauthorised modification of data held in a computer; or

(iii) any unauthorised impairment of electronic communication to or from a computer; and

(b) the unauthorised access, modification or impairment is caused by means of a telecommunications service; and

(c) the person knows the access, modification or impairment is unauthorised; and

(d) the person intends to commit, or facilitate the commission of, a serious offence against a law of the Commonwealth, a State or a Territory (whether by that person or another person) by the access, modification or impairment.

(2) Absolute liability applies to paragraph (1)(b).

(3) In a prosecution for an offence against subsection (1), it is not necessary to prove that the defendant knew that the offence was:
  (a) an offence against a law of the Commonwealth, a State or a Territory; or
  (b) a serious offence.

Intention to commit a serious Commonwealth offence

(4) A person is guilty of an offence if:
  (a) the person causes:
    (i) any unauthorised access to data held in a computer; or
    (ii) any unauthorised modification of data held in a computer; or
    (iii) any unauthorised impairment of electronic communication to or from a computer; and
  (b) the person knows the access, modification or impairment is unauthorised; and
  (c) the person intends to commit, or facilitate the commission of, a serious offence against a law of the Commonwealth (whether by that person or another person) by the access, modification or impairment.

(5) In a prosecution for an offence against subsection (3), it is not necessary to prove that the defendant knew that the offence was:
  (a) an offence against a law of the Commonwealth; or
  (b) a serious offence.

Penalty

(6) A person who is guilty of an offence against this section is punishable, on conviction, by a penalty not exceeding the penalty applicable to the serious offence.

Impossibility

(7) A person may be found guilty of an offence against this section even if committing the serious offence is impossible.

No offence of attempt

(8) It is not an offence to attempt to commit an offence against this section.

*Meaning of **serious offence***

(9) In this section:

serious offence means an offence that is punishable by imprisonment for life or a period of 5 or more years.

477.2 Unauthorised modification of data to cause impairment

(1) A person is guilty of an offence if:
  (a) the person causes any unauthorised modification of data held in a computer; and
  (b) the person knows the modification is unauthorised; and
  (c) the person is reckless as to whether the modification impairs or will impair:
    (i) access to that or any other data held in any computer; or
    (ii) the reliability, security or operation, of any such data; and
  (d) one or more of the following applies:

(i) the data that is modified is held in a Commonwealth computer;
(ii) the data that is modified is held on behalf of the Commonwealth in a computer;
(iii) the modification of the data is caused by means of a telecommunications service;
(iv) the modification of the data is caused by means of a Commonwealth computer;
(v) the modification of the data impairs access to, or the reliability, security or operation of, other data held in a Commonwealth computer;
(vi) the modification of the data impairs access to, or the reliability, security or operation of, other data held on behalf of the Commonwealth in a computer;
(vii) the modification of the data impairs access to, or the reliability, security or operation of, other data by means of a telecommunications service.

Penalty: 10 years imprisonment.

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

(3) A person may be guilty of an offence against this section even if there is or will be no actual impairment to:
(a) access to data held in a computer; or
(b) the reliability, security or operation, of any such data.

(4) A conviction for an offence against this section is an alternative verdict to a charge for an offence against section 477.3 (unauthorised impairment of electronic communication).

477.3 Unauthorised impairment of electronic communication

(1) A person is guilty of an offence if:
(a) the person causes any unauthorised impairment of electronic communication to or from a computer; and
(b) the person knows that the impairment is unauthorised; and
(c) one or both of the following applies:
(i) the electronic communication is sent to or from the computer by means of a telecommunications service;
(ii) the electronic communication is sent to or from a Commonwealth computer.

Penalty: 10 years imprisonment.

(2) Absolute liability applies to paragraph (1)(c).

(3) A conviction for an offence against this section is an alternative verdict to a charge for an offence against section 477.2 (unauthorised modification of data to cause impairment).

Division 478—Other computer offences

478.1 Unauthorised access to, or modification of, restricted data

(1) A person is guilty of an offence if:
(a) the person causes any unauthorised 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 unauthorised; 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.

478.2 Unauthorised impairment of data held on a computer disk etc.

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

(a) the person causes any unauthorised impairment of the reliability, security or operation of data held on:

(i) a computer disk; or

(ii) a credit card; or

(iii) another device used to store data by electronic means; and

(b) the person intends to cause the impairment; and

(c) the person knows that the impairment is unauthorised; and

(d) the computer disk, credit card or other device is owned or leased by a Commonwealth entity.

Penalty: 2 years imprisonment.

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

478.3 Possession or control of data with intent to commit a computer offence

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

(a) the person has possession or control of data; and

(b) the person has that possession or control with the intention that the data be used, by the person or another person, in:

(i) committing an offence against Division 477; or

(ii) facilitating the commission of such an offence.

Penalty: 3 years imprisonment.

(2) A person may be found guilty of an offence against this section even if committing the offence against Division 477 is impossible.

No offence of attempt

(3) It is not an offence to attempt to commit an offence against this section.

Meaning of possession or control of data

(4) In this section, a reference to a person having possession or control of data includes a reference to the person:

(a) having possession of a computer or data storage device that holds or contains the data; or

(b) having possession of a document in which the data is recorded; or

(c) having control of data held in a computer that is in the possession of another person (whether inside or outside Australia).

478.4 Producing, supplying or obtaining data with intent to commit a computer offence

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

(a) the person produces, supplies or obtains data; and

(b) the person does so with the intention that the data be used, by the person or another person, in:

(i) committing an offence against Division 477; or

(ii) facilitating the commission of such an offence.

Penalty: 3 years imprisonment.

(2) A person may be found guilty of an offence against this section even if committing the offence against Division 477 is impossible.

No offence of attempt

(3) It is not an offence to attempt to commit an offence against this section.

Meaning of producing, supplying or obtaining data

(4) In this section, a reference to a person producing, supplying or obtaining data includes a reference to the person:

(a) producing, supplying or obtaining data held or contained in a computer or data storage device; or

(b) producing, supplying or obtaining a document in which the data is recorded.

Canada:

Making, having or dealing in instruments for forging or falsifying credit cards -- s. 342.01(1)

342.01 (1) Every person who, without lawful justification or excuse,
(a) makes or repairs,
(b) buys or sells,
(c) exports from or imports into Canada, or
(d) possesses
any instrument, device, apparatus, material or thing that the person knows has been used or knows is adapted or intended for use in forging or falsifying credit cards is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

Forfeiture -- s. 342.01(2)

(2) Where a person is convicted of an offence under subsection (1), any instrument, device, apparatus, material or thing in relation to which the offence was committed or the possession of which constituted the offence may, in addition to any other punishment that may be imposed, be ordered forfeited to Her Majesty, whereupon it may be disposed of as the Attorney General directs.

Limitation -- s. 342.01(3)

(3) No order of forfeiture may be made under subsection (2) in respect of any thing that is the property of a person who was not a party to the offence under subsection (1).

1997, c. 18, s. 17.

Unauthorized use of computer -- s. 342.1(1)

342.1 (1) Every one who, fraudulently and without colour 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, or
(d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a 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, or is guilty of an offence punishable on summary conviction.

Definitions -- s. 342.1(2)

(2) In this section,

"computer password"

"computer password" means any data by which a computer service or computer system is capable of being obtained or used;

"computer program"

"computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

"computer service"

"computer service" includes data processing and the storage or retrieval of data;

"computer system"

"computer system" means a device that, or a group of interconnected or related devices one or more of which,

(a) contains computer programs or other data, and

(b) pursuant to computer programs,

(i) performs logic and control, and

(ii) may perform any other function;

"data"

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system;

"electro-magnetic, acoustic, mechanical or other device"

"electro-magnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;

"function"

"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system;

"intercept"

"intercept" includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof.

"traffic"

"traffic" means, in respect of a computer password, to sell, export from or import into Canada, distribute or deal with in any other way.

R.S., 1985, c. 27 (1st Supp.), s. 45; 1997, c. 18, s. 18.

Possession of device to obtain computer service -- s. 342.2(1)

342.2 (1) Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section,

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or

(b) is guilty of an offence punishable on summary conviction.

Forfeiture -- s. 342.2(2)

(2) Where a person is convicted of an offence under subsection (1), any instrument or device, in relation to which the offence was committed or the possession of which constituted the offence, may, in addition to any other punishment that may be imposed, be ordered forfeited to Her Majesty, whereupon it may be disposed of as the Attorney General directs.

Limitation -- s. 342.2(3)

(3) No order of forfeiture may be made under subsection (2) in respect of any thing that is the property of a person who was not a party to the offence under subsection (1).

1997, c. 18, s. 19.

WILLFULLY CAUSING EVENT TO OCCUR - Colour of right - Interest
Section 429

(1) Every one who causes the occurrence of an event by doing an act or by omitting to do an act that is his duty to do, knowing that the act or omission will probably cause the occurrence of the event and being reckless whether the event occurs or not, shall be deemed, for the purpose of this Part, willfully to have caused the occurrence of the event.
(2) No person shall be convicted of an offence under sections 430 to 446 where he proves that he acted with legal justification or excuse and with colour of right.

Mischief -- ss. 430 to 432
Mischief -- s. 430(1)
430. (1) Every one commits mischief who wilfully
(a) destroys or damages property;
(b) renders property dangerous, useless, inoperative or ineffective;
(c) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property; or
(d) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property.
Mischief in relation to data -- s. 430(1.1)
(1.1) Every one commits mischief who wilfully
(a) destroys or alters data;
(b) renders data meaningless, useless or ineffective;
(c) obstructs, interrupts or interferes with the lawful use of data; or
(d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.
Punishment -- s. 430(2)
(2) Every one who commits mischief that causes actual danger to life is guilty of an indictable offence and liable to imprisonment for life.
Punishment -- s. 430(3)
(3) Every one who commits mischief in relation to property that is a testamentary instrument or the value of which exceeds five thousand dollars
(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or
(b) is guilty of an offence punishable on summary conviction.
Idem -- s. 430(4)
(4) Every one who commits mischief in relation to property, other than property described in subsection (3),
(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or
(b) is guilty of an offence punishable on summary conviction.
Idem -- s. 430(5)
(5) Every one who commits mischief in relation to data
(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or
(b) is guilty of an offence punishable on summary conviction.
Offence -- s. 430(5.1)
(5.1) Every one who wilfully does an act or wilfully omits to do an act that it is his duty to do, if that act or omission is likely to constitute mischief causing actual danger to life, or to constitute mischief in relation to property or data,
(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years; or
(b) is guilty of an offence punishable on summary conviction.
Saving -- s. 430(6)
(6) No person commits mischief within the meaning of this section by reason only that
(a) he stops work as a result of the failure of his employer and himself to agree on any matter relating to his employment;
(b) he stops work as a result of the failure of his employer and a bargaining agent acting on his behalf to agree on any matter relating to his employment; or
(c) he stops work as a result of his taking part in a combination of workmen or employees for their own reasonable protection as workmen or employees.
Idem -- s. 430(7)
(7) No person commits mischief within the meaning of this section by reason only that he attends at or near or approaches a dwelling-house or place for the purpose only of obtaining or communicating information.

Definition of "data" -- s. 430(8)
(8) In this section, "data" has the same meaning as in section 342.1.
R.S., 1985, c. C-46, s. 430; R.S., 1985, c. 27 (1st Supp.), s. 57; 1994, c. 44, s. 28.

Germany:

Section 202a

Data espionage
(1) Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment not exceeding three years or a fine.
(2) Within the meaning of subsection (1) above data shall only be those stored or transmitted electronically or
magnetically or otherwise in a manner not immediately perceivable.
Section 202b
Phishing
Whosoever unlawfully intercepts data (section 202a(2)) not intended for him, for himself or another by technical means from a non-public data processing facility or from the electromagnetic broadcast of a data
processing facility, shall be liable to imprisonment not exceeding two years or a fine, unless the offence incurs
a more severe penalty under other provisions.
Section 202c
Acts preparatory to data espionage and phishing
(1) Whosoever prepares the commission of an offence under section 202a or section 202b by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible
1. passwords or other security codes enabling access to data (section 202a(2)), or
2. software for the purpose of the commission of such an offence,
shall be liable to imprisonment not exceeding one year or a fine.

(2) Section 149(2) and (3) shall apply mutatis mutandis.

Section 263a
Computer fraud
(1) Whosoever with the intent of obtaining for himself or a third person an unlawful material benefit damages
the property of another by influencing the result of a data processing operation through incorrect configuration
of a program, use of incorrect or incomplete data, unauthorised use of data or other unauthorised influence on
the course of the processing shall be liable to imprisonment not exceeding five years or a fine.
(2) Section 263(2) to (7) shall apply mutatis mutandis.
(3) Whosoever prepares an offence under subsection (1) above by writing computer programs the purpose of
which is to commit such an act, or procures them for himself or another, offers them for sale, or holds or supplies them to another shall be liable to imprisonment not exceeding three years or a fine.

(4) In cases under subsection (3) above section 149(2) and (3) shall apply mutatis mutandis.

Section 303a
Data tampering
(1) Whosoever unlawfully deletes, suppresses, renders unusable or alters data (section 202a (2)) shall be

liable to imprisonment not exceeding two years or a fine.
(2) The attempt shall be punishable.

Section 303b

Computer sabotage

(1) Whosoever interferes with data processing operations which are of substantial importance to another by
1. committing an offence under section303a(1); or
2. entering or transmitting data (section 202a(2)) with the intention of causing damage to another; or
3. destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier,
shall be liable to imprisonment not exceeding three years or a fine.
(2) If the data processing operation is of substantial importance for another's business, enterprise or a public
authority, the penalty shall be imprisonment not exceeding five years or a fine.
(3) The attempt shall be punishable.
(4) In especially serious cases under subsection (2) above the penalty shall be imprisonment from six months
to ten years. An especially serious case typically occurs if the offender
1. causes major financial loss,
2. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of computer sabotage, or
3. through the offence jeopardises the population's supply with vital goods or services or the national security of the Federal Republic of Germany.
(5) Section 202c shall apply mutatis mutandis to acts preparatory to an offence under subsection (1) above.

Section 303c

Request to prosecute

In cases under sections 303 to 303b the offence may only be prosecuted upon request, unless the prosecuting authority considers propio motu that prosecution is required because of special public interest.

England & Wales:

35 Unauthorised access to computer material
(1) In the Computer Misuse Act 1990 (c. 18) ("the 1990 Act"), section 1 (offence of unauthorised 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;
(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."
36 Unauthorised acts with intent to impair operation of computer, etc

For section 3 of the 1990 Act (unauthorised modification of computer material) there is substituted-
"3 Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

(1) A person is guilty of an offence if-
(a) he does any unauthorised act in relation to a computer;
(b) at the time when he does the act he knows that it is unauthorised; and

(c) either subsection (2) or subsection (3) below applies.
(2) This subsection applies if the person intends by doing the act-
(a) to impair the operation of any computer;
(b) to prevent or hinder access to any program or data held in any computer;
(c) to impair the operation of any such program or the reliability of any such data; or
(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.
(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above.
(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to-
(a) any particular computer;
(b) any particular program or data; or
(c) a program or data of any particular kind.
(5) In this section-
(a) a reference to doing an act includes a reference to causing an act to be done;
(b) "act" includes a series of acts;
(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.
(6) 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 ten years or to a fine or to both."

37 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.
(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."

38 Transitional and saving provision
(1) The amendments made by-
(a) subsection (2) of section 35, and
(b) paragraphs 19(2), 25(2) and 29(2) of Schedule 14,
apply only where every act or other event proof of which is required for conviction of an offence under section 1 of the 1990 Act takes place after that subsection comes into force.
(2) The amendments made by-
(a) subsection (3) of section 35, and
(b) paragraphs 23, 24, 25(4) and (5), 26, 27(2) and (7) and 28 of Schedule 14,
do not apply in relation to an offence committed before that subsection comes into force.
(3) An offence is not committed under the new section 3 unless every act or other event proof of which is required for conviction of the offence takes place after section 36 above comes into force.
(4) In relation to a case where, by reason of subsection (3), an offence is not committed under the new

section 3-
(a) section 3 of the 1990 Act has effect in the form in which it was enacted;
(b) paragraphs 19(3), 25(3) to (5), 27(4) and (5) and 29(3) and (4) of Schedule 14 do not apply.
(5) An offence is not committed under the new section 3A unless every act or other event proof of which is required for conviction of the offence takes place after section 37 above comes into force.
(6) In the case of an offence committed before section 154(1) of the Criminal Justice Act 2003 (c. 44) comes into force, the following provisions have effect as if for "12 months" there were substituted "six months"-
(a) paragraph (a) of the new section 1(3);
(b) paragraph (a) of the new section 2(5);
(c) subsection (6)(a) of the new section 3;
(d) subsection (5)(a) of the new section 3A.
(7) In this section-
(a) "the new section 1(3)" means the subsection (3) substituted in section 1 of the 1990 Act by section 35 above;
(b) "the new section 2(5)" means the subsection (5) substituted in section 2 of the 1990 Act by paragraph 17 of Schedule 14 to this Act;
(c) "the new section 3" means the section 3 substituted in the 1990 Act by section 36 above;
(d) "the new section 3A" means the section 3A inserted in the 1990 Act by section 37 above.
Computer Misuse Act 1990
Chapter 18

1. Unauthorized access to computer material:
(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, or to enable any such access to be secured,
(b) the access he intends to secure, or to enable to be secured, 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 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.

2. Unauthorized access with intent to commit or facilitate commission for further offences.
(1) 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 (whether by himself or by any other person); and the offense he intends to commit or facilitate is referred to below in this section as the further offense.
(2) 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 (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the Magistrates Courts Act 1980).
(3) 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.
(4) 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.
(5) 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.

3 Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.
(1) A person is guilty of an offence if-
(a) he does any unauthorised act in relation to a computer;
(b) at the time when he does the act he knows that it is unauthorised; and
(c) either subsection (2) or subsection (3) below applies.
(2) This subsection applies if the person intends by doing the act-
(a) to impair the operation of any computer;
(b) to prevent or hinder access to any program or data held in any computer;
(c) to impair the operation of any such program or the reliability of any such data; or
(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.
(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above.
(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to-
(a) any particular computer;
(b) any particular program or data; or
(c) a program or data of any particular kind.
(5) In this section-
(a) a reference to doing an act includes a reference to causing an act to be done;
(b) "act" includes a series of acts;
(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.
(6) 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 ten years or to a fine or to both.

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.
(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.

Ireland:

Criminal Justice (Theft and Fraud Offences) Act 2001
Section 9 - Unlawful use of computer
(1) A person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another, is guilty of an offence.

(2) A person guilty of an offence under this section is liable on conviction on indictment to a fine or imprisonment for a term not exceeding 10 years or both.

Criminal Damages Act 1991
Section 5 – Unauthorised accessing of data
(1) A person who without lawful excuse operates a computer -
(a) within the State with intent to access any data kept either within or outside the State, or:
(b) outside the State with intent to access any data kept within the State, shall, whether or not he accesses any data, be guilty of an offense and shall be liable on summary conviction to a fine not exceeding £500 or imprisonment for a term not exceeding 3 months or both.
(2) Subsection (1) applies whether or not the person intended to access any particular data or any category of data or data kept by any particular person.

Mexico:

Penal Code Part 9

Chapter II
Articles 211 bis 1: Whoever without authorization modifies, destroys or causes loss of information contained in computer systems or computer equipments protected by security measures, shall be liable to imprisonment for a term of six months to two years and to fines of one hundre to three hundred days.
Whoever without authorization obtains access to or copies information contained in computer systems or computer equipments protected by security measures, shall be liable to imprisonment for a term of three months to one year and to fines of fifty to one hundred and fifty days.
Articles 211 bis 2: Whoever without authorization modifies, destroys or causes loss of information contained in governmental computer systems or computer equipments protected by security measures, shall be liable to imprisonment for a term of one year to four years and to fines of one hundred to six hundred days.
Whoever without authorization obtains access to or copies information contained in governmental computer systems or equipments protected by security measures, shall be liable to imprisonment for a term of six months to two years and fines of one hundred to three hundred days.
Article 211 bis 4: Whoever without authorization modifies, destroys or causes loss of information contained in computer systems or computer equipments of institutions as part of the financial system protected by security measures, shall be liable to imprisonment for a term of six months to four years and fines of one hundred to six hundred days.
Whoever without authorization obtains access to or copies information contained in computer systems or computer equipments of institutions as part of the financial system protected by security measures, shall be liable to imprisonment for a term of three months to two years and fines of fifty to three hundred days.

New Zealand:

Crimes Amendment Act 2003 No 39 Part 1 s 15, of July 7th

‘Crimes involving computers
‘‘248 Interpretation
For the purposes of this section and sections 249 and 250,—
‘‘access, in relation to any computer system, means instruct, communicate with, store data in, receive data from, or otherwise make use of any of the resources of the computer system
‘‘computer system—

‘‘(a) means—
‘‘(i) a computer; or
‘‘(ii) 2 or more interconnected computers; or
‘‘(iii) any communication links between computers or to remote terminals or another device; or
‘‘(iv) 2 or more interconnected computers combined with any communication links between computers or to remote terminals or any other device;
and
‘‘(b) includes any part of the items described in paragraph (a) and all related input, output, processing, storage, software, or communication facilities, and stored data.
‘‘249 Accessing computer system for dishonest purpose
‘‘(1) Every one is liable to imprisonment for a term not exceeding 7 years who, directly or indirectly, accesses any computer system and thereby, dishonestly or by deception, and without claim of right,—
‘‘(a) obtains any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or
‘‘(b) causes loss to any other person.
‘‘(2) Every one is liable to imprisonment for a term not exceeding 5 years who, directly or indirectly, accesses any computer system with intent, dishonestly or by deception, and without claim of right,—
‘‘(a) to obtain any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or
‘‘(b) to cause loss to any other person.
‘‘(3) In this section, deception has the same meaning as in section 240(2).
250 Damaging or interfering with computer system
‘‘(1) Every one is liable to imprisonment for a term not exceeding 10 years who intentionally or recklessly destroys, damages, or alters any computer system if he or she knows or ought to know that danger to life is likely to result.
‘‘(2) Every one is liable to imprisonment for a term not exceeding 7 years who intentionally or recklessly, and without authorisation, knowing that he or she is not authorised, or being reckless as to whether or not he or she is authorised,—
‘‘(a) damages, deletes, modifies, or otherwise interferes with or impairs any data or software in any computer system;
or
‘‘(b) causes any data or software in any computer system to be damaged, deleted, modified, or otherwise interfered with or impaired; or
‘‘(c) causes any computer system to—
‘‘(i) fail; or
‘‘(ii) deny service to any authorised users.

‘‘251 Making, selling, or distributing or possessing software for committing crime
‘‘(1) Every one is liable to imprisonment for a term not exceeding 2 years who invites any other person to acquire from him or her, or offers or exposes for sale or supply to any other person, or agrees to sell or supply or sells or supplies to any other person, or has in his or her possession for the purpose of sale or supply to any other person, any software or other information that would enable another person to access a computer system without authorisation—
‘‘(a) the sole or principal use of which he or she knows to be the commission of a crime; or
‘‘(b) that he or she promotes as being useful for the commission of a crime (whether or not he or she also promotes it as being useful for any other purpose), knowing or being reckless as to whether it will be used for the commission of a crime.
‘‘(2) Every one is liable to imprisonment for a term not exceeding 2 years who—
‘‘(a) has in his or her possession any software or other information that would enable him or her to access a computer system without authorisation; and
‘‘(b) intends to use that software or other information to commit a crime.
Compare: 1961 No 43 ss 216D(1), 229, 244
‘‘252 Accessing computer system without authorisation
‘‘(1) Every one is liable to imprisonment for a term not exceeding 2 years who intentionally accesses, directly or indirectly, any computer system without authorisation, knowing that he or she is not authorised to access that computer system, or being reckless as to whether or not he or she is authorised to access that computer system.
‘‘(2) To avoid doubt, subsection (1) does not apply if a person who is authorised to access a computer system accesses that computer system for a purpose other than the one for which that person was given access.
‘‘(3) To avoid doubt, subsection (1) does not apply if access to a computer system is gained by a law enforcement agency—
‘‘(a) under the execution of an interception warrant or search warrant; or
‘‘(b) under the authority of any Act or rule of the common law.
‘‘253 Qualified exemption to access without authorisation offence for New Zealand Security Intelligence Service
Section 252 does not apply if—
‘‘(a) the person accessing a computer system is—
‘‘(i) the person specified in an interception warrant issued under the New Zealand Security Intelligence Service Act 1969; or

‘‘(ii) a person, or member of a class of persons, requested to give any assistance that is specified in that warrant; and

‘‘(b) the person accessing a computer system is doing so for the purpose of intercepting or seizing any communication, document, or thing of the kind specified in that warrant.

‘‘254 Qualified exemption to access without authorisation offence for Government Communications Security Bureau

Section 252 does not apply if the person that accesses a computer system—

‘‘(a) is authorised to access that computer system under the Government Communications Security Bureau Act 2003; and

‘‘(b) accesses that computer system in accordance with that authorisation.