

# AR Electronic Crime Statutes

([http://170.94.58.9/data/ar\\_code.asp](http://170.94.58.9/data/ar_code.asp))

## 5-41-101.

### Purpose.

It is found and determined that computer-related crime poses a major problem for business and government; that losses for each incident of computer-related crime are potentially astronomical; that the opportunities for computer-related crime in business and government through the introduction of fraudulent records into a computer system, the unauthorized use of computers, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets are great; that computer-related crime has a direct effect on state commerce; and that, while various forms of computer-related crime might possibly be the subject of criminal charges based on other provisions of law, it is appropriate and desirable that a statute be enacted which deals directly with computer-related crime.

**History.** Acts 1987, No. 908, § 1.

## 5-41-102.

### Definitions.

As used in this chapter, unless the context otherwise requires:

(1) "Access" means to instruct, communicate with, store data in, or retrieve data from a computer, computer system, or computer network;

(2) "Computer" means an electronic device that performs logical, arithmetic, and memory functions by manipulating electronic or magnetic impulses and includes all input, output, processing, storage, computer software, and communication facilities that are connected or related to that device in a system or a network;

(3) "Computer network" means the interconnection of communications lines with a computer through remote terminals or a complex consisting of two (2) or more interconnected computers;

(4) "Computer program" means a set of instructions, statements, or related data that, in actual or modified form, is capable of causing a computer or a computer system to perform specified functions;

(5) "Computer software" means one (1) or more computer programs, existing in any form, or any associated operational procedures, manuals, or other documentation;

(6) "Computer system" means a set of related, connected, or unconnected computers, other devices, and software;

(7) "Data" means any representation of information, knowledge, facts, concepts, or instructions which are being prepared or have been prepared and are intended to be processed or stored, are being processed or stored, or have been processed or stored in a computer, computer network, or computer system;

(8) "Financial instrument" includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computer system representation thereof;

(9) In this subchapter, "message" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature, or any transfer of a computer program.

(10) "Property" includes, but is not limited to, financial instruments, data, computer programs, documents associated with computers and computer programs, or copies thereof, whether tangible or intangible, including both human and computer readable data, and data while in transit;

(11) "Services" includes, but is not limited to, the use of a computer, a computer system, a computer network, computer software, a computer program, or data.

**History.** Acts 1987, No. 908, § 2; 1997, No. 1153, § 1.

**5-41-103. Computer fraud.**

(a) Any person commits computer fraud who intentionally accesses or causes to be accessed any computer, computer system, computer network, or any part thereof for the purpose of:

(1) Devising or executing any scheme or artifice to defraud or extort; or

(2) Obtaining money, property, or services with false or fraudulent intent, representations, or promises.

(b) Computer fraud is a Class D felony.

**History.** Acts 1987, No. 908, § 3.

**5-41-104.**

**Computer**

**trespass.**

(a) Any person commits computer trespass who intentionally and without authorization accesses, alters, deletes, damages, destroys, or disrupts any computer, computer system, computer network, computer program, or data.

(b) Computer trespass is a Class C misdemeanor if it is a first violation which does not cause any loss or damage.

(c) Computer trespass is a Class B misdemeanor if:

(1) It is a second or subsequent violation which does not cause any loss or damage;  
or

(2) It is a violation which causes loss or damage of less than five hundred dollars (\$500).

(d) Computer trespass is a Class A misdemeanor if it is a violation which causes loss or damage of five hundred dollars (\$500) or more, but less than two thousand five hundred dollars (\$2,500).

(e) Computer trespass is a Class D felony if it is a violation which causes loss or damage of two thousand five hundred dollars (\$2,500) or more.

**History.** Acts 1987, No. 908, § 4.

**5-41-105.**

**Venue**

**of**

**violations.**

For the purpose of venue under this chapter, any violation of this chapter shall be considered to have been committed in any county:

(1) In which any act was performed in furtherance of any course of conduct which violated this chapter;

(2) In which any violator had control or possession of any proceeds of the violation or of any books, records, documents, property, financial instrument, computer software, computer program, data, or other material or objects which were used in furtherance of the violation;

(3) From which, to which, or through which any access to a computer or computer network was made whether by wires, electromagnetic waves, microwaves, or any other means of communication;

(4) In which any computer, computer system, or computer network is an object or an instrument of the violation is located at the time of the alleged violation.

**History.** Acts 1987, No. 908, § 5.

**5-41-106. Civil actions.**

(a) Any person whose property or person is injured by reason of a violation of any provision of this chapter may sue therefor and recover for any damages sustained and the costs of suit. Without limiting the generality of the term, "damages" shall include loss of profits.

(b) At the request of any party to an action brought pursuant to this section, the court, in its discretion, may conduct all legal proceedings in such a way as to protect the secrecy and security of the computer, computer system, computer network, computer program, computer software, and data involved in order to prevent possible reoccurrence of the same or a similar act by another person and to protect any trade secrets of any party.

(c) No civil action under this section may be brought except within three (3) years from the date the alleged violation of this chapter is discovered or should have been discovered by the exercise of reasonable diligence.

**History.** Acts 1987, No. 908, § 6.

**5-41-107. Assistance of Attorney General.**

If requested to do so by a prosecuting attorney, the Attorney General may assist the prosecuting attorney in the investigation or prosecution of an offense under this chapter or any other offense involving the use of a computer.

**History.** Acts 1987, No. 908, § 7.

**5-41-108. Unlawful computerized communications.**

(a)(1) A person commits the offense of unlawful computerized communications if:

(A) With the purpose to frighten, intimidate, threaten, abuse, or harass another person, he sends a message to the person on an electronic mail or other computerized communication system and in that message threatens to cause physical injury to any person or damage to the property of any person; or

(B) With the purpose to frighten, intimidate, threaten, abuse, or harass another person, he sends a message on an electronic mail or other computerized communication system with the reasonable expectation that the person will receive the message and in that message threatens to cause physical injury to any person or damage to the property of any person; or

(C) With the purpose to frighten, intimidate, threaten, abuse, or harass another person, he sends a message to another person on an electronic mail or other computerized communication system and in that message uses any obscene, lewd, or profane language; or

(D) With the purpose to frighten, intimidate, threaten, abuse, or harass another person, he sends a message on an electronic mail or other computerized communication system with the reasonable expectation that the person will receive the message and in that message uses any obscene, lewd, or profane language.

(2) Unlawful computerized communications is a Class A misdemeanor.

(b)(1) The judicial officer in a court of competent jurisdiction shall upon pretrial release of the defendant enter an order consistent with Rules 9.3 and 9.4 of the Arkansas Rules of Criminal Procedure and shall give notice to defendant of penalties contained in Rule 9.5 of the Arkansas Rules of Criminal Procedure.

(2) This protective order shall remain in effect during the pendency of any appeal of a conviction under this section.

**History.** Acts 1997, No. 1153, § 2.

**5-41-109. Disclosure of personal information.**

An Internet service provider shall disclose personally identifiable information concerning a consumer pursuant to a subpoena, warrant, or court order issued under authority of a law of this state, another state, or the United States Government.

**History.** Acts 2003, No. 1087, § 6.

**5-41-201. Definitions.**

For purposes of this subchapter:

(1) "Access" means to intercept, instruct, communicate with, store data in, retrieve from, or otherwise make use of any resources of a computer, network, or data;

(2)(A) "Computer" means an electronic, magnetic, electrochemical, or other high-speed data-processing device performing logical, arithmetic, or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with the device.

(B) "Computer" also includes any on-line service, Internet service, local bulletin board, any electronic storage device, including a floppy disk or other magnetic storage device, or any compact disk that has read-only memory and the capacity to store audio, video, or written materials;

(3)(A) "Computer contaminant" means any data, information, image, program, signal, or sound that is designed or has the capability to:

(i) Contaminate, corrupt, consume, damage, destroy, disrupt, modify, record, or transmit; or

(ii) Cause to be contaminated, corrupted, consumed, damaged, destroyed, disrupted, modified, recorded, or transmitted any other data, information, image, program, signal, or sound contained in a computer, system, or network without the knowledge or consent of the person who owns the other data, information, image, program, signal, or sound or the computer, system, or network.

(B) "Computer contaminant" includes, but is not limited to:

(i) A virus, worm, or Trojan horse; or

(ii) Any other similar data, information, image, program, signal, or sound that is designed or has the capability to prevent, impede, delay, or disrupt the normal operation or use of any component, device, equipment, system, or network;

(4) "Data" means a representation of any form of information, knowledge, facts, concepts, or instructions which is being prepared or has been formally prepared and is intended to be processed, is being processed, or has been processed in a system or network;

(5) "Encryption" means the use of any protection or disruptive measure, including, without limitation, cryptography, enciphering, encoding, or a computer contaminant to:

(A) Prevent, impede, delay, or disrupt access to any data, information, image, program, signal, or sound;

(B) Cause or make any data, information, image, program, signal, or sound unintelligible or unusable; or

(C) Prevent, impede, delay, or disrupt the normal operation or use of any component, device, equipment, system, or network;

(6) "Information service" means a service that is designed or has the capability to generate, process, store, retrieve, convey, emit, transmit, receive, relay, record, or reproduce any data, information, image, program, signal, or sound by means of any

component, device, equipment, system, or network, including, but not limited to, by means of:

(A) A computer, computer system, computer network, modem, or scanner;

(B) A telephone, cellular phone, satellite phone, pager, personal communications device, or facsimile machine;

(C) Any type of transmitter or receiver; or

(D) Any other component, device, equipment, system, or network that uses analog, digital, electronic, electromagnetic, magnetic, or optical technology;

(7)(A) "Network" means a set of related, remotely connected devices and facilities, including more than one (1) system, with the capability to transmit data among any of the devices and facilities.

(B) "Network" includes, but is not limited to, a local, regional, or global computer network;

(8) "Program" means an ordered set of data representing coded instructions or statements which can be executed by a computer and cause the computer to perform one (1) or more tasks;

(9) "Property" means anything of value and includes a financial instrument, information, electronically produced data, program, and any other tangible or intangible item of value;

(10) "Provider" means any person who provides an information service;

(11) "Provider of Internet service" means any provider who provides subscribers with access to the Internet or an electronic mail address, or both; and

(12) "System" means a set of related equipment, whether or not connected, which is used with or for a computer.

**History.** Acts 2001, No. 1496, § 2.

**5-41-202. Unlawful acts regarding computers.**

(a) A person commits an unlawful act regarding a computer if the person knowingly and without authorization:

(1) Modifies, damages, destroys, discloses, uses, transfers, conceals, takes, retains possession of, copies, obtains or attempts to obtain access to, permits access to or causes to be accessed, or enters data or a program which exists inside or outside a computer, system, or network;

(2) Modifies, destroys, uses, takes, damages, transfers, conceals, copies, retains possession of, obtains or attempts to obtain access to, permits access to or causes to be accessed, equipment or supplies that are used or intended to be used in a computer, system, or network;

(3) Destroys, damages, takes, alters, transfers, discloses, conceals, copies, uses, retains possession of, obtains or attempts to obtain access to, permits access to or causes to be accessed, a computer, system, or network;

(4) Obtains and discloses, publishes, transfers, or uses a device used to access a computer, network, or data; or

(5) Introduces, causes to be introduced, or attempts to introduce a computer contaminant into a computer, system, or network.

(b) An unlawful act regarding a computer is a Class A misdemeanor.

(c) An unlawful act regarding a computer shall be a Class C felony if the act:

(1) Was committed to devise or execute a scheme to defraud or illegally obtain property;

(2) Caused damage in excess of five hundred dollars (\$500); or

(3) Caused an interruption or impairment of a public service, including, without limitation, a governmental operation, a system of public communication or transportation, or a supply of water, gas, or electricity.

**History.** Acts 2001, No. 1496, § 2.

**5-41-203. Unlawful interference with access to computers - Unlawful use  
or access of computers.**

(a)(1) A person commits unlawful interference with access to computers if the person knowingly and without authorization interferes with, denies, or causes the denial of access to or use of a computer, system, or network to a person who has the duty and right to use it.

(2) Unlawful interference with access to computers is a Class A misdemeanor.

(b)(1) A person commits unlawful use or access to computers if the person knowingly and without authorization uses, causes the use of, accesses, attempts to gain access to, or causes access to be gained to a computer, system, network, telecommunications device, telecommunications service, or information service.

(2) Unlawful use or access to computers is a Class A misdemeanor.

(c) If the violation of subsection (a) or (b) of this section was committed to devise or execute a scheme to defraud or illegally obtain property, the person is guilty of a Class C felony.

(d)(1) It is an affirmative defense to a charge made pursuant to this section that at the time of the alleged offense the person reasonably believed that:

(A) The person was authorized to use or access the computer, system, network, telecommunications device, telecommunications service, or information service and the use or access by the person was within the scope of that authorization; or

(B) The owner or other person authorized to give consent would authorize the person to use or access the computer, system, network, telecommunications device, telecommunications service, or information service.

(2) A person who intends to offer an affirmative defense provided in subdivision (d)(1) of this section at a trial or preliminary hearing shall file and serve on the prosecuting attorney a notice of that intent not fewer than fourteen (14) calendar days before the trial or hearing or at such other time as the court may direct.

**History.** Acts 2001, No. 1496, § 2.

**5-41-204. Unlawful use of encryption.**

(a) A person commits unlawful use of encryption if the person knowingly uses or attempts to use encryption, directly or indirectly, to:

(1) Commit, facilitate, further, or promote any criminal offense;

(2) Aid, assist, or encourage another person to commit any criminal offense;

(3) Conceal the commission of any criminal offense;

(4) Conceal or protect the identity of a person who has committed any criminal offense; or

(5) Delay, hinder, or obstruct the administration of the law.

(b) A person who violates any provision of this section commits a criminal offense that is separate and distinct from any other criminal offense and may be prosecuted and convicted pursuant to this section whether or not the person or any other person is or has been prosecuted or convicted for any other criminal offense arising out of the same facts as the violation of this section.

(c)(1) An unlawful use of encryption is a Class D felony if the criminal offense concealed by encryption is a Class Y, Class A, or Class B felony.

(2) An unlawful use of encryption is a Class A misdemeanor if the criminal offense concealed by encryption is a Class C or Class D felony, or an unclassified felony.

(3) Any other unlawful use of encryption shall be a misdemeanor classed one (1) degree below the misdemeanor constituted by the criminal offense concealed by encryption.

**History.** Acts 2001, No. 1496, § 2.

**5-41-205. Unlawful acts involving electronic mail.**

(a) A person commits an unlawful act involving electronic mail if, with the purpose to devise or execute a scheme to defraud or illegally obtain property, the person:

(1) Knowingly and with the purpose to transmit or cause to be transmitted the item of electronic mail to the electronic mail address of one (1) or more recipients without their knowledge of or consent to the transmission falsifies or forges any data, information, image, program, signal, or sound that:

(A) Is contained in the header, subject line, or routing instructions of an item of electronic mail; or

(B) Describes or identifies the sender, source, point of origin, or path of transmission of an item of electronic mail;

(2) Purposely transmits or causes to be transmitted an item of electronic mail to the electronic mail address of one (1) or more recipients without their knowledge of or consent to the transmission, if the person knows or has reason to know that the item of electronic mail contains or has been generated or formatted with:

(A) An Internet domain name that is being used without the consent of the person who holds the Internet domain name; or

(B) Any data, information, image, program, signal, or sound that has been used intentionally in the header, subject line, or routing instructions of the item of electronic mail to falsify or misrepresent:

(i) The identity of the sender; or

(ii) The source, point of origin, or path of transmission of the item of electronic mail;  
or

(3) Knowingly sells, gives, or otherwise distributes or possesses with the intent to sell, give, or otherwise distribute any data, information, image, program, signal, or sound which is designed or intended to be used to falsify or forge any data, information, image, program, signal, or sound that:

(A) Is contained in the header, subject line, or routing instructions of an item of electronic mail; or

(B) Describes or identifies the sender, source, point of origin, or path of transmission of an item of electronic mail.

(b) Subdivision (a)(2) of this section does not apply to a provider of Internet service who, in the course of providing service, transmits or causes to be transmitted an item of electronic mail on behalf of another person, unless the provider of Internet service is the person who first generates the item of electronic mail.

(c) An unlawful act involving electronic mail is a Class D felony.

**History.** Acts 2001, No. 1496, § 2.

**5-41-206. Computer password disclosure.**

(a) A person commits computer password disclosure if the person purposely and without authorization discloses a number, code, password, or other means of access to a computer or computer network.

(b) Computer password disclosure is a Class A misdemeanor.

(c) If the violation of subsection (a) of this section was committed to devise or execute a scheme to defraud or illegally obtain property, the person is guilty of a Class D felony.

**History.** Acts 2001, No. 1496, § 2.