

WV Electronic Crime Statutes

(<http://www.legis.state.wv.us/>)

ARTICLE 3C. WEST VIRGINIA COMPUTER CRIME AND ABUSE ACT.

§61-3C-1. Short title.

This act shall be known and may be cited as the "West Virginia Computer Crime and Abuse Act."

61-3C-2. Legislative findings.

The Legislature finds that:

- (a) The computer and related industries play an essential role in the commerce and welfare of this state.
- (b) Computer-related crime is a growing problem in business and government.
- (c) Computer-related crime has a direct effect on state commerce and can result in serious economic and, in some cases, physical harm to the public.
- (d) Because of the pervasiveness of computers in today's society, opportunities are great for computer related crimes through the introduction of false records into a computer or computer system, the unauthorized use of computers and computer facilities, the alteration and destruction of computers, computer programs and computer data, and the theft of computer resources, computer software and computer data.
- (e) Because computers have now become an integral part of society, the Legislature recognizes the need to protect the rights of owners and legitimate users of computers and computer systems, as well as the privacy interest of the general public, from those who abuse computers and computer systems.
- (f) While various forms of computer crime or abuse might possibly be the subject of criminal charges or civil suit based on other provisions of law, it is appropriate and desirable that a supplemental and additional statute be provided which specifically proscribes various forms of computer crime and abuse and provides criminal penalties and civil remedies therefor.

§61-3C-3. Definitions.

As used in this article, unless the context clearly indicates otherwise:

- (a) "Access" means to instruct, communicate with, store data in, retrieve data from, intercept data from or otherwise make use of any computer, computer network, computer program, computer software, computer data or other computer resources.
- (b) "Authorization" means the express or implied consent given by a person to another to access or use said person's computer, computer network, computer program, computer software, computer system, password, identifying code or personal identification number.
- (c) "Computer" means an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic or storage functions and includes any data storage facility or communication facility directly related to or operating in conjunction with such device. The term "computer" includes any connected or directly related device, equipment or facility which enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or another device, but such term does not include an automated

typewriter or typesetter, a portable hand-held calculator or other similar device.

(d) "Computer contaminant" means any set of computer instructions that are designed to damage or destroy information within a computer, computer system or computer network without the consent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources or damage or destroy the normal operation of the computer.

(e) "Computer data" means any representation of knowledge, facts, concepts, instruction or other information computed, classified, processed, transmitted, received, retrieved, originated, stored, manifested, measured, detected, recorded, reproduced, handled or utilized by a computer, computer network, computer program or computer software and may be in any medium, including, but not limited to, computer print-outs, microfilm, microfiche, magnetic storage media, optical storage media, punch paper tape or punch cards, or it may be stored internally in read-only memory or random access memory of a computer or any other peripheral device.

(f) "Computer network" means a set of connected devices and communication facilities, including more than one computer, with the capability to transmit computer data among them through such communication facilities.

(g) "Computer operations" means arithmetic, logical, storage, display, monitoring or retrieval functions or any combination thereof and includes, but is not limited to, communication with, storage of data in or to, or retrieval of data from any device and the human manual manipulation of electronic magnetic impulses. A "computer operation" for a particular computer shall also mean any function for which that computer was designed.

(h) "Computer program" means an ordered set of computer data representing instructions or statements, in a form readable by a computer, which controls, directs or otherwise influences the functioning of a computer or computer network.

(i) "Computer software" means a set of computer programs, procedures and associated documentation concerned with computer data or with the operation of a computer, computer program or computer network.

(j) "Computer services" means computer access time, computer data processing or computer data storage and the computer data processed or stored in connection therewith.

(k) "Computer supplies" means punch cards, paper tape, magnetic tape, magnetic disks or diskettes, optical disks or diskettes, disk or diskette packs, paper, microfilm and any other tangible input, output or storage medium used in connection with a computer, computer network, computer data, computer software or computer program.

(l) "Computer resources" includes, but is not limited to, information retrieval; computer data processing, transmission and storage; and any other functions performed, in whole or in part, by the use of a computer, computer network, computer software or computer program.

- (m) "Owner" means any person who owns or leases or is a licensee of a computer, computer network, computer data, computer program, computer software, computer resources or computer supplies.
- (n) "Person" means any natural person, general partnership, limited partnership, trust, association, corporation, joint venture or any state, county or municipal government and any subdivision, branch, department or agency thereof.
- (o) "Property" includes:
- (1) Real property;
 - (2) Computers and computer networks;
 - (3) Financial instruments, computer data, computer programs, computer software and all other personal property regardless of whether they are:
 - (i) Tangible or intangible;
 - (ii) In a format readable by humans or by a computer;
 - (iii) In transit between computers or within a computer network or between any devices which comprise a computer; or
 - (iv) Located on any paper or in any device on which it is stored by a computer or by a human; and
 - (4) Computer services.
- (p) "Value" means having any potential to provide any direct or indirect gain or advantage to any person.
- (q) "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 computerized representation thereof.
- (r) "Value of property or computer services" shall be: (1) The market value of the property or computer services at the time of a violation of this article; or (2) if the property or computer services are unrecoverable, damaged or destroyed as a result of a violation of section six or seven of this article, the cost of reproducing or replacing the property or computer services at the time of the violation.

§61-3C-4. Computer fraud; access to Legislature computer; criminal penalties.

(a) Any person who, knowingly and willfully, directly or indirectly, accesses or causes to be accessed any computer, computer services or computer network for the purpose of (1) executing any scheme or artifice to defraud or (2) obtaining money, property or services by means of fraudulent pretenses, representations or promises is guilty of a felony, and, upon conviction thereof, shall be fined not more than ten thousand dollars or imprisoned in the penitentiary for not more than ten years, or both fined and imprisoned.

(b)(1) Any person who, knowingly and willfully, directly or indirectly, accesses, attempts to access, or causes to be accessed any data stored in a computer owned by the Legislature without authorization is guilty of a felony, and, upon conviction thereof, shall be fined not more than five thousand dollars or imprisoned in the penitentiary for not more than five years, or both fined and imprisoned.

(2) Notwithstanding the provisions of section seventeen of this article to the contrary, in any criminal prosecution under this subsection against an employee

or member of the Legislature, it shall not be a defense (A) that the defendant had reasonable grounds to believe that he or she had authorization to access the data merely because of his or her employment or membership, or (B) that the defendant could not have reasonably known he or she did not have authorization to access the data: *Provided*, That the joint committee on government and finance shall promulgate rules for the respective houses of the Legislature regarding appropriate access of members and staff and others to the legislative computer system.

§61-3C-5. Unauthorized access to computer services.

Any person who knowingly, willfully and without authorization, directly or indirectly, accesses or causes to be accessed a computer or computer network with the intent to obtain computer services shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not less than two hundred dollars nor more than one thousand dollars or confined in the county jail not more than one year, or both.

§61-3C-6. Unauthorized possession of computer data or programs.

(a) Any person who knowingly, willfully and without authorization possesses any computer data or computer program belonging to another and having a value of five thousand dollars or more shall be guilty of a felony, and, upon conviction thereof, shall be fined not more than ten thousand dollars or imprisoned in the penitentiary for not more than ten years, or both.

(b) Any person who knowingly, willfully and without authorization possesses any computer data or computer program belonging to another and having a value of less than five thousand dollars shall be guilty of a misdemeanor, and, upon conviction thereof shall be fined not more than one thousand dollars or confined in the county jail for not more than one year, or both.

§61-3C-7. Alteration, destruction, etc., of computer equipment.

(a) *Misdemeanor offenses.* -- Any person who knowingly, willfully and without authorization, directly or indirectly, tampers with, deletes, alters, damages or destroys or attempts to tamper with, delete, alter, damage or destroy any computer, computer network, computer software, computer resources, computer program or computer data or who knowingly introduces, directly or indirectly, a computer contaminant into any computer, computer program or computer network which results in a loss of value of property or computer services up to one thousand dollars, is guilty of a misdemeanor and, upon conviction thereof, shall be fined not more than one thousand dollars or confined in the county or regional jail not more than six months, or both.

(b) *Felony offenses.* -- Any person who knowingly, willfully and without authorization, directly or indirectly, damages or destroys or attempts to damage or destroy any computer, computer network, computer software, computer resources, computer program or computer data by knowingly introducing, directly or indirectly, a computer contaminant into any computer, computer program or computer network which results in a loss of value of property or computer services more than one thousand dollars is guilty of a felony and, upon conviction thereof, shall be fined not less than two hundred dollars and not more than ten thousand dollars or confined in a state correctional facility not more than ten

years, or both, or, in the discretion of the court, be fined not less than two hundred nor more than one thousand dollars and confined in the county or regional jail not more than one year.

§61-3C-8. Disruption of computer services.

Any person who knowingly, willfully and without authorization, directly or indirectly, disrupts or degrades or causes the disruption or degradation of computer services or denies or causes the denial of computer services to an authorized recipient or user of such computer services, shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not less than two hundred nor more than one thousand dollars or confined in the county jail not more than one year, or both.

§61-3C-9. Unauthorized possession of computer information, etc.

Any person who knowingly, willfully and without authorization, possesses any computer data, computer software, computer supplies or a computer program which he knows or reasonably should know was obtained in violation of any section of this article shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not less than two hundred nor more than one thousand dollars or confined in the county jail for not more than one year, or both.

§61-3C-10. Disclosure of computer security information.

Any person who knowingly, willfully and without authorization discloses a password, identifying code, personal identification number or other confidential information about a computer security system to another person shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not more than five hundred dollars or confined in the county jail for not more than six months, or both.

§61-3C-11. Obtaining confidential public information.

Any person who knowingly, willfully and without authorization accesses or causes to be accessed any computer or computer network and thereby obtains information filed by any person with the state or any county or municipality which is required by law to be kept confidential shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not more than five hundred dollars or confined in the county jail not more than six months, or both.

§61-3C-12. Computer invasion of privacy.

Any person who knowingly, willfully and without authorization accesses a computer or computer network and examines any employment, salary, credit or any other financial or personal information relating to any other person, after the time at which the offender knows or reasonably should know that he is without authorization to view the information displayed, shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not more than five hundred dollars or confined in the county jail for not more than six months, or both.

§61-3C-13. Fraud and related activity in connection with access devices.

(a) As used in this section, the following terms shall have the following meanings:
(1) "Access device" means any card, plate, code, account number, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated

solely by paper instrument);

(2) "Counterfeit access device" means any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device;

(3) "Unauthorized access device" means any access device that is lost, stolen, expired, revoked, canceled, or obtained without authority;

(4) "Produce" includes design, alter, authenticate, duplicate, or assemble;

(5) "Traffic" means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of.

(b) Any person who knowingly and willfully possesses any counterfeit or unauthorized access device shall be guilty of a misdemeanor, and, upon conviction thereof, shall be fined not more than one thousand dollars or confined in the county jail for not more than six months, or both.

(c) Any person who knowingly, willfully and with intent to defraud possesses a counterfeit or unauthorized access device or who knowingly, willfully and with intent to defraud, uses, produces or traffics in any counterfeit or unauthorized access device shall be guilty of a felony, and, upon conviction thereof, shall be fined not more than ten thousand dollars or imprisoned in the penitentiary not more than ten years, or both.

(d) This section shall not prohibit any lawfully authorized investigative or protective activity of any state, county or municipal law-enforcement agency.

§61-3C-14. Endangering public safety.

Any person who accesses a computer or computer network and knowingly, willfully and without authorization (a) interrupts or impairs the providing of services by any private or public utility; (b) interrupts or impairs the providing of any medical services; (c) interrupts or impairs the providing of services by any state, county or local government agency, public carrier or public communication service; or otherwise endangers public safety shall be guilty of a felony, and, upon conviction thereof, shall be fined not more than fifty thousand dollars or imprisoned not more than twenty years, or both.

§61-3C-14a. Obscene, anonymous, harassing and threatening communications by computer; penalty.

(a) It is unlawful for any person, with the intent to harass or abuse another person, to use a computer to:

(1) Make contact with another without disclosing his or her identity with the intent to harass or abuse;

(2) Make contact with a person after being requested by the person to desist from contacting them;

(3) Threaten to commit a crime against any person or property; or

(4) Cause obscene material to be delivered or transmitted to a specific person after being requested to desist from sending such material.

For purposes of this section, "obscene material" means material that:

(A) An average person, applying contemporary adult community standards, would find, taken as a whole, appeals to the prurient interest, is intended to appeal to the prurient interest, or is pandered to a prurient interest;

(B) An average person, applying contemporary adult community standards,

would find, depicts or describes, in a patently offensive way, sexually explicit conduct consisting of an ultimate sexual act, normal or perverted, actual or simulated, an excretory function, masturbation, lewd exhibition of the genitals, or sadomasochistic sexual abuse; and

(C) A reasonable person would find, taken as a whole, lacks literary, artistic, political or scientific value.

(b) It is unlawful for any person to knowingly permit a computer under his or her control to be used for any purpose prohibited by this section.

(c) Any offense committed under this section may be determined to have occurred at the place at which the contact originated or the place at which the contact was received or intended to be received.

(d) Any person who violates a provision of this section is guilty of a misdemeanor and, upon conviction thereof, shall be fined not more than five hundred dollars or confined in a county or regional jail not more than six months, or both. For a second or subsequent offense, the person is guilty of a misdemeanor and, upon conviction thereof, shall be fined not more than one thousand dollars or confined in a county or regional jail for not more than one year, or both.

§61-3C-14b. Soliciting, etc. a minor via computer; penalty.

Any person over the age of eighteen, who knowingly uses a computer to solicit, entice, seduce or lure, or attempt to solicit, entice, seduce or lure, a minor known or believed to be at least four years younger than the person using the computer or a person he or she believes to be such a minor, to commit any illegal act proscribed by the provisions of article eight, eight-b, eight-c or eight-d of this chapter, or any felony offense under section four hundred one, article four, chapter sixty-a of this code, is guilty of a felony and, upon conviction thereof, shall be fined not more than five thousand dollars or imprisoned in a state correctional facility not less than two nor more than ten years, or both.

§61-3C-15. Computer as instrument of forgery.

The creation, alteration or deletion of any computer data contained in any computer or computer network, which if done on a tangible document or instrument would constitute forgery under section five, article four, chapter sixty-one of this code will also be deemed to be forgery. The absence of a tangible writing directly created or altered by the offender shall not be a defense to any crime set forth in section five, article four, chapter sixty-one if a creation, alteration or deletion of computer data was involved in lieu of a tangible document or instrument.

61-3C-16. Civil relief; damages.

(a) Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefor in circuit court and may be entitled to recover for each violation:

(1) Compensatory damages;

(2) Punitive damages; and

(3) Such other relief, including injunctive relief, as the court may deem appropriate.

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 may, in its discretion, conduct all legal proceedings in such a manner as to protect the secrecy and security of the computer network, computer data, computer program or computer software involved in order to prevent any possible recurrence of the same or a similar act by another person or to protect any trade secret or confidential information of any person. For the purposes of this section "trade secret" means the whole or any portion or phase of any scientific or technological information, design, process, procedure or formula or improvement which is secret and of value. A trade secret shall be presumed to be secret when the owner thereof takes measures to prevent it from becoming available to persons other than those authorized by the owner to have access thereto for a limited purpose.

(c) The provisions of this section shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.

(d) A civil action under this section must be commenced before the earlier of: (1) Five years after the last act in the course of conduct constituting a violation of this article; or (2) two years after the plaintiff discovers or reasonably should have discovered the last act in the course of conduct constituting a violation of this article.

§61-3C-17. Defenses to criminal prosecution.

(a) In any criminal prosecution under this article, it shall be a defense that:

(1) The defendant had reasonable grounds to believe that he had authority to access or could not have reasonably known he did not have authority to access the computer, computer network, computer data, computer program or computer software in question; or,

(2) The defendant had reasonable grounds to believe that he had the right to alter or destroy the computer data, computer software or computer program in question; or,

(3) The defendant had reasonable grounds to believe that he had the right to copy, reproduce, duplicate or disclose the computer data, computer program, computer security system information or computer software in question.

(b) Nothing in this section shall be construed to limit any defense available to a person charged with a violation of this article.

§61-3C-18. Venue.

For the purpose of criminal and civil venue under this article, any violation of this article shall be considered to have been committed:

(1) In any county in which any act was performed in furtherance of any course of conduct which violates this article;

(2) In the county of the principal place of business in this state of the aggrieved owner of the computer, computer data, computer program, computer software or computer network, or any part thereof;

(3) In any county in which any violator had control or possession of any proceeds of the violation or any books, records, documentation, property, financial instrument, computer data, computer software, computer program, or other material or objects which were used in furtherance of or obtained as a result of the violation;

(4) In any county 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; and
(5) In the county in which the aggrieved owner or the defendant resides or either of them maintains a place of business.

§61-3C-19. Prosecution under other criminal statutes not prohibited.

Criminal prosecution pursuant to this article shall not prevent prosecution pursuant to any other provision of law.

§61-3C-20. Personal jurisdiction.

Any person who violates any provision of this article and, in doing so, accesses, permits access to, causes access to or attempts to access a computer, computer network, computer data, computer resources, computer software or computer program which is located, in whole or in part, within this state, or passes through this state in transit, shall be subject to criminal prosecution and punishment in this state and to the civil jurisdiction of the courts of this state.

§61-3C-21. Severability.

If any provision of this article or the application thereof to any person or circumstance is held invalid, such invalidity shall not affect any other provisions or applications of this article which can be given effect without the invalid provision or application, and to that end the provisions of this article are declared to be severable.

ARTICLE 6G. ELECTRONIC MAIL PROTECTION ACT.

§46A-6G-1. Definitions.

As used in this article:

(1) "Bulk electronic mail message" means an electronic mail message sent in bulk to users of an interactive computer service who have not requested or solicited the message. Unauthorized for purposes of a bulk electronic mail message, means a bulk electronic mail message sent in quantity in contravention of the authorization granted by or in violation of the policies or contractual rights of the electronic mail service provider.

(2) "Electronic mail address" means a destination, commonly expressed as a string of characters, to which electronic mail may be sent or delivered.

(3) "Initiate the transmission" means the action by the original sender of an electronic mail message, not the action by any intervening interactive computer service that may handle or retransmit the message.

(4) "Interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the internet.

(5) "Internet domain name" means a globally unique, hierarchical reference to an internet host or service, assigned through centralized internet naming authorities, comprising a series of character strings separated by periods, with the right-most string specifying the top of the hierarchy.

(6) "Person" means any individual, corporation, partnership, association, limited liability company or any other form or business association.

§46A-6G-2. Limitations on unauthorized electronic mail.

No person may initiate the transmission of an unauthorized electronic mail message with the intent to deceive and defraud, or a bulk electronic mail message from a computer located in the state of West Virginia or to an electronic mail address that the sender knows, or has reason to know, is held by a West Virginia resident that:

- (1) Uses a third party's internet domain name without the permission of the third party, or otherwise misrepresents any information in identifying the point of origin or the transmission path of a commercial electronic mail message;
- (2) Contains false or misleading information in the subject line;
- (3) Does not clearly provide the date and time the message is sent, the identity of the person sending the message, and the return electronic mail address of that person; or
- (4) Contains "sexually explicit materials" which are defined as a visual depiction, in actual or simulated form, or an explicit description in a predominately sexual context, nudity, human genitalia, or any act of natural or unnatural sexual intercourse.

§46A-6G-3. Interactive computer service authority; liability.

(1) An interactive computer service may block the receipt or transmission through its service of any bulk electronic mail that it reasonably believes is, or will be, sent in violation of this article.

(2) An interactive computer service may disconnect or terminate the service of any person that is in violation of this article.

(3) No interactive computer service may be held liable for any action voluntarily taken in good faith to block the receipt or transmission through its service of any bulk electronic mail which it reasonably believes is, or will be, sent in violation of this article; nor will any interactive computer service be held liable for any action voluntarily taken in good faith to disconnect or terminate the service of any person that is in violation of this article.

(4) No interactive computer service or public utility will be liable for merely transmitting a bulk electronic mail message on its network.

§46A-6G-4. Sale or possession of enabling software prohibited.

No person may sell, give or otherwise distribute or possess with the intent to sell, give or distribute software that:

(1) Is primarily designed or produced for the purpose of facilitating or enabling the falsification of electronic mail transmission information or other routing information;

(2) Has only a limited commercially significant purpose or use other than to facilitate or enable the falsification of electronic mail transmission information or other routing information; or

(3) That is marketed by that person or another acting in concert with that person with that person's knowledge for use in facilitating or enabling the falsification of electronic mail transmission information or other routing information.

§46A-6G-5. Violations; right of action for injunction, damages.

(a) No person or organization may initiate an unauthorized bulk electronic mail message in violation of this article.

(b) A recipient of an unauthorized bulk electronic mail message in violation of this article may bring an action to recover actual damages for any injury sustained by the receipt of an unauthorized bulk electronic mail message. In lieu of actual damages, a minimum damage assessment of one thousand dollars may be recovered for violations of this article. Punitive damages may be awarded for the willful failure to cease initiating unauthorized bulk electronic mail messages. Court costs and reasonable attorney fees may be awarded for violations of this article.

(c) A recipient of an unauthorized bulk electronic mail message initiated in violation of this article may bring an action to enjoin the initiator from sending any further unauthorized bulk electronic mail messages. Any court costs or other costs incident to such action including reasonable attorney fees may be awarded.

(d) Initiating an unauthorized bulk electronic mail message to any computer or computer network located in this state shall constitute an act in the state for the purposes of section thirty-three, article three, chapter fifty-six of this code.

(e) Any interactive computer service provider or public utility whose property or person is injured by any violation of this article may bring an action to recover for any damages sustained, including, but not limited to, loss of profits. In addition, court costs and attorney fees may be recovered. The service provider may elect, in lieu of actual damages, to recover ten dollars for each and every unauthorized bulk electronic mail message transmitted in violation of this article, or twenty-five thousand dollars per day, whichever is greater.

(f) The provisions of this section shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.