

# SC Electronic Crime Statutes

<http://www.scstatehouse.net/code/statmast.htm>

## Title 16 - Crimes and Offenses

### CHAPTER 16.

#### COMPUTER CRIME ACT

#### SECTION 16-16-10. Definitions.

For purposes of this chapter:

- (a) "Computer" means a device that performs logical, arithmetic, and memory functions by manipulating impulses including, but not limited to, all input, output, processing, storage, computer software, and communication facilities that are connected or related to a computer in a computer system or computer network. For the purposes of this section, "computer" includes, but is not limited to, mainframes, servers, workstations, desktops, and notebooks; industrial controls such as programmable logic controllers and supervisory control and data acquisition systems; portable hand-held computing devices such as personal digital assistants and digital cellular telephones; data communications network devices such as routers and switches; and all other devices that are computer-based or communicate with or are under the control of a computer such as appropriate telephone switches, medical devices, and cable and satellite television interface systems. "Computer" does not include automated typewriters or typesetters.
- (b) "Computer network" means the interconnection of two or more computers, and those devices and facilities through which an interconnection occurs.
- (c) "Computer program" means a series of instructions or statements executable on a computer, which direct the computer system in a manner to process data or perform other specified functions.
- (d) "Computer software" means a set of computer programs, data, procedures, or associated documentation concerned with the operation of a computer system.
- (e) "Computer system" means a set of related, whether connected or unconnected, computer equipment, devices, or software.
- (f) "Property" includes, but is not limited to, financial instruments, data, documents associated with computer systems, and computer software, or copies thereof, whether tangible or intangible, including both human and computer system readable data, and data while in transit.
- (g) "Services" include, but are not limited to, the use of the computer system, computer network, computer programs, or data prepared for computer use, or data obtained within a computer system, or data contained within a computer network.

(h) "Data" means a representation of information, knowledge, facts, concepts, or instructions that has been prepared or is being prepared in a formalized manner and has been processed, is being processed, or is intended to be processed in a computer, computer system, or computer network. Data may be in any form including, but not limited to, computer printouts, magnetic storage media, optical storage media, network data packets, flash memory cards, smart card memory, punched cards, or as stored in the memory of the computer or in transit or displayed on a video device.

(i) "Access" means to gain entry to, attempt to gain entry to, instruct, communicate with, attempt to communicate with, store or alter data in, retrieve or remove data from, or otherwise make use of or attempt to make use of the logical, arithmetic, control, memory, storage, output, or communication functions of a computer, computer system, or computer network.

(j) "Computer hacking" means:

(1) accessing or attempting to access all or part of a computer, computer system, or a computer network without express or implied authorization for the purpose of establishing contact only;

(2) with the intent to defraud or with malicious intent to commit a crime after the contact is established;

(3) misusing computer or network services including, but not limited to, mail transfer programs, file transfer programs, proxy servers, and web servers by performing functions not authorized by the appropriate principal of the computer, computer system, or computer network. Misuse of computer and network services includes, but is not limited to, the unauthorized use of:

(i) mail transfer programs to send mail to persons other than the authorized users of that computer or computer network;

(ii) file transfer program proxy services or proxy servers to access other computers, computer systems, or computer networks; and

(iii) web servers to redirect users to other web pages or web servers;

(4) using a group of computer programs commonly known as "port scanners" or "probes" to intentionally access any computer, computer system, or computer network without the permission of the appropriate principal of the computer, computer system, or computer network. This group of computer programs includes, but is not limited to, those computer programs that use a computer network to access a computer, computer system, or another computer network to determine:

(i) the presence or types of computers or computer systems on a network;

- (ii) the computer network's facilities and capabilities;
- (iii) the availability of computer or network services;
- (iv) the presence or versions of computer software including, but not limited to, operating systems, computer services, or computer contaminants;
- (v) the presence of a known computer software deficiency that can be used to gain unauthorized access to a computer, computer system, or computer network; or
- (vi) any other information about a computer, computer system, or computer network not necessary for the normal and lawful operation of the computer initiating the access.

This group of computer programs does not include standard computer software used for the normal operation, administration, management, and test of a computer, computer system, or computer network including, but not limited to, operating system services such as domain name services and mail transfer services, network monitoring and management computer software such as the computer programs commonly called "ping", "tcpdump", and "traceroute", and systems administration computer software such as the computer programs commonly known as "nslookup" and "whois". It is unlawful to intentionally and knowingly use such computer software to access any computer, computer system, or computer network to adversely affect computer or network access or performance; and

- (5) the intentional use of a computer, computer system, or a computer network in a manner that exceeds any right or permission granted by the appropriate principal of the computer, computer system, or computer network.

Computer hacking does not include the introduction of a computer contaminant into a computer, computer system, computer program, or computer network.

(k) "Computer contaminant" means a computer program designed to modify, damage, destroy, disable, deny or degrade access to, allow unauthorized access to, functionally impair, record, or transmit information within a computer, computer system, or computer network without the express or implied consent of the owner. Computer contaminant includes, but is not limited to:

(1) a group of computer programs commonly known as "viruses" and "worms" that are self-replicating or self-propagating, and that are designed to contaminate other computer programs, compromise computer security, consume computer resources, modify, destroy, record, or transmit data, or disrupt the normal operation of the computer, computer system, or computer network;

(2) a group of computer programs commonly known as "Trojans" or "Trojan horses" that are not self-replicating or self-propagating, and that are designed to compromise computer security, consume computer resources, modify, destroy, record, or transmit

data, or disrupt the normal operation of the computer, computer system, or computer network;

(3) a group of computer programs commonly known as "zombies" that are designed to use a computer without the knowledge and consent of the appropriate principal, and that are designed to send large quantities of data to a targeted computer network for the purpose of degrading the targeted computer's or network's performance, or denying access through the network to the targeted computer or network, resulting in what is commonly known as "Denial of Service" or "Distributed Denial of Service" attacks; or

(4) a group of computer programs commonly known as "trap doors", "back doors", or "root kits" that are designed to bypass standard authentication software, and that are designed to allow access to or use of a computer without the knowledge or consent of the appropriate principal.

(l) "Unauthorized access" means access of a computer, computer system, or computer network not explicitly or implicitly authorized by the appropriate principal of the computer, computer system, or computer network.

(m) "Unauthorized use" means the:

(i) use of a computer, computer system, or computer network not explicitly or implicitly authorized by the appropriate principal of the computer, computer system, or computer network;

(ii) the use of computer software not explicitly or implicitly authorized by the appropriate principal or licensee of the computer software; or

(iii) the authorized use of a computer, computer system, computer network, or computer software in a manner not explicitly or implicitly authorized by the appropriate principal or licensee.

**SECTION 16-16-20. Computer crime offenses; penalties.**

(1) It is unlawful for a person to wilfully, knowingly, maliciously, and without authorization or for an unauthorized purpose to:

(a) directly or indirectly access or cause to be accessed a computer, computer system, or computer network for the purpose of:

(i) devising or executing a scheme or artifice to defraud;

(ii) obtaining money, property, or services by means of false or fraudulent pretenses, representations, promises; or

(iii) committing any other crime.

(b) alter, damage, destroy, or modify a computer, computer system, computer network, computer software, computer program, or data contained in that computer, computer system, computer program, or computer network or introduce a computer contaminant into that computer, computer system, computer program, or computer network.

(2) A person is guilty of computer crime in the first degree if the amount of gain directly or indirectly derived from the offense made unlawful by subsection (1) or the loss directly or indirectly suffered by the victim exceeds ten thousand dollars. Computer crime in the first degree is a felony and, upon conviction, a person must be fined not more than fifty thousand dollars or imprisoned not more than five years, or both.

(3)(a) A person is guilty of computer crime in the second degree if the amount of gain directly or indirectly derived from the offense made unlawful by subsection (1) or the loss directly or indirectly suffered by the victim is greater than one thousand dollars but not more than ten thousand dollars.

(b) A person is also guilty of computer crime in the second degree where:

(i) he interferes with, causes to be interfered with, denies or causes to be denied any computer or network service to an authorized user of the computer or network service for the purpose of devising or executing any scheme or artifice to defraud, or obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises, or committing any other felony;

(ii) he deprives the owner of possession of, or takes, transfers, conceals, or retains possession of any computer, data, computer property, or computer-related property, including all parts of a computer, computer system, computer network, computer software, computer services, or information associated with a computer, whether in a tangible or intangible form; or

(iii) the gain derived from the offense made unlawful by subsection (1) or loss suffered by the victim cannot reasonably be ascertained.

(c) Computer crime in the second degree is a misdemeanor and, upon conviction for a first offense, a person must be fined not more than ten thousand dollars or imprisoned not more than one year, or both. Upon conviction for a second or subsequent offense, a person is guilty of a misdemeanor and must be fined not more than twenty thousand dollars or imprisoned not more than two years, or both.

(4) A person is guilty of computer crime in the third degree if the amount of gain directly or indirectly derived from the offense made unlawful by subsection (1) or the loss directly or indirectly suffered by the victim is not more than one thousand dollars. A person is also guilty of computer crime in the third degree if he wilfully, knowingly, and without authorization or for an unauthorized purpose engages in computer hacking. Computer crime in the third degree is a misdemeanor and, upon conviction for a first offense, a person must be fined not more than two hundred dollars or imprisoned not

more than thirty days. Upon conviction for a second or subsequent offense, a person must be fined not more than two thousand dollars or imprisoned not more than two years, or both.

(5) Each computer, computer system, or computer network affected by the violation of this chapter constitutes a separate violation.

**SECTION 16-16-25.** Compensatory damages and restitution.

In addition to other civil remedies available, the owner or lessee of a computer, computer system, computer network, computer program, or data may bring a civil action against a person convicted under this chapter for compensatory damages, restitution, and attorney's fees. Compensatory damages and restitution may include:

- (1) expenditures reasonably and necessarily incurred by the owner or lessee to verify whether a computer system, computer network, computer program, or data was altered, damaged, or deleted by the access;
- (2) costs of repairing or, if necessary, replacing the affected computer, computer system, computer network, computer software, computer program, or data;
- (3) lost profits for the period that the computer, computer system, computer network, computer software, computer program, or data was unusable; and
- (4) costs of replacing or restoring the data lost or damaged as a result of a violation of this chapter.

**SECTION 16-16-30.** Venue.

For the purpose of venue under this chapter, a violation of this chapter is considered to have been committed in the county in which the violation took place; however, upon proper motion and the proper showing before a judge, venue may be transferred if justice would be better served by the transfer, to one of the following:

- (1) a county in which an act was performed in furtherance of a transaction which violated this chapter;
- (2) the county of the principal place of business in this State of the owner or lessee of a computer, computer system, computer network, or any part of it, which has been subject to the violation; or
- (3) a county in which a violator had control or possession of proceeds of the violation or of books, records, documents, property, financial instruments, computer software, computer programs, or other materials or objects which were used in the furtherance of the violation.

**SECTION 16-16-40.** Applicability of other criminal law provisions.

The provisions of this chapter must not be construed to preclude the applicability of any other provision of the criminal law of this State, which presently applies or may in the future apply, to any transaction which violates this chapter.