

UT Electronic Crime Statutes

(<http://www.le.state.ut.us/~code/code.htm>)

76-6-701. Computer Crimes Act -- Short title.

This part is known as the "Utah Computer Crimes Act."

76-6-702. Definitions.

As used in this part:

(1) "Access" means to directly or indirectly use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, computer network, or any means of communication with any of them.

(2) "Authorization" means having the express or implied consent or permission of the owner, or of the person authorized by the owner to give consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission.

(3) "Computer" means any electronic device or communication facility that stores, retrieves, processes, or transmits data.

(4) "Computer system" means a set of related, connected or unconnected, devices, software, or other related computer equipment.

(5) "Computer network" means:

(a) the interconnection of communication or telecommunication lines between:

(i) computers; or

(ii) computers and remote terminals; or

(b) the interconnection by wireless technology between:

(i) computers; or

(ii) computers and remote terminals.

(6) "Computer property" includes electronic impulses, electronically produced data, information, financial instruments, software, or programs, in either machine or human readable form, any other tangible or intangible item relating to a computer, computer system, computer network, and copies of any of them.

(7) "Confidential" means data, text, or computer property that is protected by a security system that clearly evidences that the owner or custodian intends that it not be available to others without the owner's or custodian's permission.

(8) "Information" does not include information obtained:

(a) through use of:

(i) an electronic product identification or tracking system; or

(ii) other technology used by a retailer to identify, track, or price goods; and

(b) by a retailer through the use of equipment designed to read the electronic product identification or tracking system data located within the retailer's location.

(9) "License or entitlement" includes:

(a) licenses, certificates, and permits granted by governments;

(b) degrees, diplomas, and grades awarded by educational institutions;

(c) military ranks, grades, decorations, and awards;

- (d) membership and standing in organizations and religious institutions;
- (e) certification as a peace officer;
- (f) credit reports; and
- (g) another record or datum upon which a person may be reasonably expected to rely in making decisions that will have a direct benefit or detriment to another.

(10) "Security system" means a computer, computer system, network, or computer property that has some form of access control technology implemented, such as encryption, password protection, other forced authentication, or access control designed to keep out

unauthorized persons.

(11) "Services" include computer time, data manipulation, and storage functions.

(12) "Financial instrument" includes any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, electronic fund transfer, automated clearing house transaction, credit card, or marketable security.

(13) "Software" or "program" means a series of instructions or statements in a form acceptable to a computer, relating to the operations of the computer, or permitting the functioning of a computer system in a manner designed to provide results including system control programs, application programs, or copies of any of them.

Amended by Chapter 72, 2005 General Session

76-6-703. Computer crimes and penalties.

(1) A person who without authorization gains or attempts to gain access to and alters, damages, destroys, discloses, or modifies any computer, computer network, computer property, computer system, computer program, computer data or software, and thereby causes damage to another, or obtains money, property, information, or a benefit for any person without legal right, is guilty of:

(a) a class B misdemeanor when:

(i) the damage caused or the value of the money, property, or benefit obtained or sought to be obtained is less than \$300; or

(ii) the information obtained is not confidential;

(b) a class A misdemeanor when the damage caused or the value of the money, property, or benefit obtained or sought to be obtained is or exceeds \$300 but is less than \$1,000;

(c) a third degree felony when the damage caused or the value of the money, property, or benefit obtained or sought to be obtained is or exceeds \$1,000 but is less than \$5,000;

(d) a second degree felony when the damage caused or the value of the money, property, or benefit obtained or sought to be obtained is or exceeds \$5,000; or

(e) a third degree felony when:

(i) the property or benefit obtained or sought to be obtained is a license or entitlement;

(ii) the damage is to the license or entitlement of another person; or

(iii) the information obtained is confidential; or

(iv) in gaining access the person breaches or breaks through a security system.

(2) (a) Except as provided in Subsection (2)(b), a person who intentionally or knowingly and without authorization gains or attempts to gain access to a computer, computer network, computer property, or computer system under circumstances not otherwise constituting an offense under this section is guilty of a class B misdemeanor.

(b) Notwithstanding Subsection (2)(a), a retailer that uses an electronic product identification or tracking system, or other technology to identify, track, or price goods is not guilty of a violation of Subsection (2)(a) if the equipment designed to read the electronic product identification or tracking system data and used by the retailer to identify, track, or price goods is located within the retailer's location.

(3) A person who uses or knowingly allows another person to use any computer, computer network, computer property, or computer system, program, or software to devise or execute any artifice or scheme to defraud or to obtain money, property, services, or other things of value by false pretenses, promises, or representations, is guilty of an offense based on the value of the money, property, services, or things of value, in the degree set forth in Subsection **76-10-1801(1)**.

(4) A person who intentionally or knowingly and without authorization, interferes with or interrupts computer services to another authorized to receive the services is guilty of a class A misdemeanor.

(5) It is an affirmative defense to Subsections (1) and (2) that a person obtained access or attempted to obtain access in response to, and for the purpose of protecting against or investigating, a prior attempted or successful breach of security of a computer, computer network, computer property, computer system whose security the person is authorized or entitled to protect, and the access attempted or obtained was no greater than reasonably necessary for that purpose.

Amended by Chapter 72, 2005 General Session

76-6-704. Attorney general, county attorney, or district attorney to prosecute -- Conduct violating other statutes.

(1) The attorney general, district attorney, or the county attorney shall prosecute suspected criminal violations of this part.

(2) Prosecution under this part does not prevent any prosecutions under any other law.

Amended by Chapter 38, 1993 General Session

76-6-705. Reporting violations.

Every person, except those to whom a statutory or common law privilege applies, who has reason to believe that the provisions of Section **76-6-703** are being or have been violated shall report the suspected violation to the attorney general, or county attorney,

or, if within a prosecution district, the district attorney of the county or prosecution district in which part or all of the violations occurred.

Amended by Chapter 38, 1993 General Session