Part 7
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, processes, transmits, or facilitates the transmission of data.

(4) "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.

(5) "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.

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

(7) "Computer technology" includes:

(a) a computer;

(b) a computer network;

(c) computer hardware;

(d) a computer system;

(e) a computer program;

(f) computer services;

(g) computer software; or

(h) computer data.

(8) "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.

(9) "Critical infrastructure" includes:

(a) a financial or banking system;

(b) any railroad, airline, airport, airway, highway, bridge, waterway, fixed guideway, or other transportation system intended for the transportation of persons or property;

(c) any public utility service, including a power, energy, gas, or water supply system;

(d) a sewage or water treatment system;

(e) a health care facility, as that term is defined in Section 26B-2-201;

(f) an emergency fire, medical, or law enforcement response system;

(g) a public health facility or system;

(h) a food distribution system;
(i) a government computer system or network;
(j) a school; or
(k) other government facilities, operations, or services.

(10) "Denial of service attack" means an attack or intrusion that is intended to disrupt legitimate access to, or use of, a network resource, a machine, or computer technology.

(11) "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.

(12)
(a) "Identifying information" means a person's:
(i) social security number;
(ii) driver license number;
(iii) nondriver governmental identification number;
(iv) bank account number;
(v) student identification number;
(vi) credit or debit card number;
(vii) personal identification number;
(viii) unique biometric data;
(ix) employee or payroll number;
(x) automated or electronic signature; or
(xi) computer password.
(b) "Identifying information" does not include information that is lawfully available from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

(13) "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.

(14) "Interactive computer service" means an information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including a service or system that provides access to the Internet or a system operated, or services offered, by a library or an educational institution.

(15) "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.

(16) "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.

(17) "Services" include computer time, data manipulation, and storage functions.
(18) "Service provider" means a telecommunications carrier, cable operator, computer hardware or software provider, or a provider of information service or interactive computer service.
(19) "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 330, 2023 General Session

76-6-703 Unlawful computer technology access or action or denial of service attack.
(1) Terms defined in Sections 76-1-101.5 and 76-6-702 apply to this section.
(2) An actor commits unlawful computer technology access or action or denial of service attack if the actor:
(a) without authorization, or in excess of the actor's authorization, accesses or attempts to access computer technology if the access or attempt to access results in:
(i) the alteration, damage, destruction, copying, transmission, discovery, or disclosure of computer technology;
(ii) interference with or interruption of:
(A) the lawful use of computer technology; or
(B) the transmission of data;
(iii) physical damage to or loss of real, personal, or commercial property;
(iv) audio, video, or other surveillance of another person; or
(v) economic loss to any person or entity;
(b) after accessing computer technology that the actor is authorized to access, knowingly takes or attempts to take unauthorized or unlawful action that results in:
(i) the alteration, damage, destruction, copying, transmission, discovery, or disclosure of computer technology;
(ii) interference with or interruption of:
(A) the lawful use of computer technology; or
(B) the transmission of data;
(iii) physical damage to or loss of real, personal, or commercial property;
(iv) audio, video, or other surveillance of another person; or
(v) economic loss to any person or entity; or
(c) knowingly engages in a denial of service attack.
(3) A violation of Subsection (2) is:
(a) a class B misdemeanor if:
(i) the economic loss or other loss or damage caused or the value of the money, property, or benefit obtained or sought to be obtained is less than $500; or
(ii) the information obtained is not confidential;
(b) a class A misdemeanor if the economic loss or other loss or damage caused or the value of the money, property, or benefit obtained or sought to be obtained is or exceeds $500 but is less than $1,500;
(c) a third degree felony if:
(i) the economic loss or other loss or damage caused or the value of the money, property, or benefit obtained or sought to be obtained is or exceeds $1,500 but is less than $5,000;
(ii) the property or benefit obtained or sought to be obtained is a license or entitlement;
(iii) the damage is to the license or entitlement of another person;

(iv) the information obtained is confidential or identifying information; or
(v) in gaining access the actor breaches or breaks through a security system; or
(d) a second degree felony if the economic loss or other loss or damage caused or the value of the money, property, or benefit obtained or sought to be obtained is or exceeds $5,000.
(4)
(a) It is an affirmative defense that the actor obtained access or attempted to obtain access:
(i) in response to, and for the purpose of protecting against or investigating, a prior attempted or successful breach of security of computer technology whose security the actor is authorized or entitled to protect, and the access attempted or obtained was no greater than reasonably necessary for that purpose; or
(ii) pursuant to a search warrant or a lawful exception to the requirement to obtain a search warrant.
(b) In accordance with 47 U.S.C. Sec. 230, this section may not apply to, and nothing in this section may be construed to impose liability or culpability on, an interactive computer service for content provided by another person.
(c) This section does not affect, limit, or apply to any activity or conduct that is protected by the constitution or laws of this state, or by the constitution or laws of the United States.
(5)
(a) An interactive computer service is not guilty of violating this section if a person violates this section using the interactive computer service and the interactive computer service did not knowingly assist the person to commit the violation.
(b) A service provider is not guilty of violating this section for:
(i) action taken in relation to a customer of the service provider, for a legitimate business purpose, to install software on, monitor, or interact with the customer's Internet or other network connection, service, or computer for network or computer security purposes, authentication, diagnostics, technical support, maintenance, repair, network management, updates of computer software or system firmware, or remote system management; or
(ii) action taken, including scanning and removing computer software, to detect or prevent the following:
(A) unauthorized or fraudulent use of a network, service, or computer software;
(B) illegal activity; or
(C) infringement of intellectual property rights.

Amended by Chapter 111, 2023 General Session

76-6-703.3 Unlawful use of technology to defraud.

(1)
(a) As used in this section, "sensitive personal identifying information" means the same as that term is defined in Section 76-6-525.
(b) Terms defined in Sections 76-1-101.5 and 76-6-702 apply to this section.
(2) An actor commits unlawful use of technology to defraud if the actor uses or knowingly allows another person to use a 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, a service, or other thing of value by a false pretense, promise, or representation.
(3) A violation of Subsection (2) is:
(a) a class B misdemeanor if the value of the money, property, service, or thing obtained or sought to be obtained is less than $500;

(b) a class A misdemeanor if the value of the money, property, service, or thing obtained or sought to be obtained is or exceeds $500 but is less than $1,500;
(c) a third degree felony if the value of the money, property, service, or thing obtained or sought to be obtained is or exceeds $1,500 but is less than $5,000; or
(d) a second degree felony if:
(i) the value of the money, property, service, or thing obtained or sought to be obtained is or exceeds $5,000; or
(ii) the object or purpose of the artifice or scheme to defraud is the obtaining of sensitive personal identifying information, regardless of the value.
(4)
(a) In accordance with 47 U.S.C. Sec. 230, this section may not apply to, and nothing in this section may be construed to impose liability or culpability on, an interactive computer service for content provided by another person.
(b) This section does not affect, limit, or apply to any activity or conduct that is protected by the constitution or laws of this state, or by the constitution or laws of the United States.
(5)
(a) An interactive computer service is not guilty of violating this section if a person violates this section using the interactive computer service and the interactive computer service did not knowingly assist the person to commit the violation.
(b) A service provider is not guilty of violating this section for:
(i) action taken in relation to a customer of the service provider, for a legitimate business purpose, to install software on, monitor, or interact with the customer's Internet or other network connection, service, or computer for network or computer security purposes, authentication, diagnostics, technical support, maintenance, repair, network management, updates of computer software or system firmware, or remote system management; or
(ii) action taken, including scanning and removing computer software, to detect or prevent the following:
(A) unauthorized or fraudulent use of a network, service, or computer software;
(B) illegal activity; or
(C) infringement of intellectual property rights.

Amended by Chapter 173, 2025 General Session

76-6-703.5 Interference or interruption of critical infrastructure.
(1) Terms defined in Sections 76-1-101.5 and 76-6-702 apply to this section.
(2) An actor commits interference or interruption of critical infrastructure if the actor intentionally or knowingly, and without lawful authorization, interferes with or interrupts critical infrastructure.
(3) A violation of Subsection (2) is a third degree felony.
(4)
(a) In accordance with 47 U.S.C. Sec. 230, this section may not apply to, and nothing in this section may be construed to impose liability or culpability on, an interactive computer service for content provided by another person.
(b) This section does not affect, limit, or apply to any activity or conduct that is protected by the constitution or laws of this state, or by the constitution or laws of the United States.
(5)
(a) An interactive computer service is not guilty of violating this section if a person violates this section using the interactive computer service and the interactive computer service did not knowingly assist the person to commit the violation.

(b) A service provider is not guilty of violating this section for:
(i) action taken in relation to a customer of the service provider, for a legitimate business purpose, to install software on, monitor, or interact with the customer's Internet or other network connection, service, or computer for network or computer security purposes, authentication, diagnostics, technical support, maintenance, repair, network management, updates of computer software or system firmware, or remote system management; or
(ii) action taken, including scanning and removing computer software, to detect or prevent the following:
(A) unauthorized or fraudulent use of a network, service, or computer software;
(B) illegal activity; or
(C) infringement of intellectual property rights.

Enacted by Chapter 111, 2023 General Session

76-6-703.7 Unlawful computer access.
(1) Terms defined in Sections 76-1-101.5 and 76-6-702 apply to this section.
(2) An actor commits unlawful computer access if:
(a) the actor intentionally or knowingly, and without authorization, gains or attempts to gain access to a computer, computer network, computer property, or computer system; and
(b) the circumstances of the violation of Subsection (2)(a) do not constitute an offense under Section 76-6-703, 76-6-703.3, 76-6-703.5, or 76-12-205.
(3) A violation of Subsection (2) is a class B misdemeanor.
(4)
(a) Notwithstanding Subsection (2), 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 this section 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.
(b) It is an affirmative defense to a violation under this section that the actor obtained access or attempted to obtain access:
(i) in response to, and for the purpose of protecting against or investigating, a prior attempted or successful breach of security of computer technology whose security the actor is authorized or entitled to protect, and the access attempted or obtained was no greater than reasonably necessary for that purpose; or
(ii) pursuant to a search warrant or a lawful exception to the requirement to obtain a search warrant.
(c) In accordance with 47 U.S.C. Sec. 230, this section may not apply to, and nothing in this section may be construed to impose liability or culpability on, an interactive computer service for content provided by another person.
(d) This section does not affect, limit, or apply to any activity or conduct that is protected by the constitution or laws of this state, or by the constitution or laws of the United States.
(5)
(a) An interactive computer service is not guilty of violating this section if an actor violates this section using the interactive computer service and the interactive computer service did not knowingly assist the actor to commit the violation.
(b) A service provider is not guilty of violating this section for:
(i) action taken in relation to a customer of the service provider, for a legitimate business purpose, to install software on, monitor, or interact with the customer's Internet or other

network connection, service, or computer for network or computer security purposes, authentication, diagnostics, technical support, maintenance, repair, network management, updates of computer software or system firmware, or remote system management; or

(ii) action taken, including scanning and removing computer software, to detect or prevent the following:

(A) unauthorized or fraudulent use of a network, service, or computer software;

(B) illegal activity; or

(C) infringement of intellectual property rights.

Amended by Chapter 173, 2025 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.

(1) Each person who has reason to believe that a provision of Section 76-6-703, 76-6-703.3, 76-6-703.5, 76-6-703.7, or 76-12-205 is being or has been violated shall report the suspected violation to:

(a) 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 violation occurred; or

(b) a state or local law enforcement agency.

(2) Subsection (1) does not apply to the extent that the person is prohibited from reporting by a statutory or common law privilege.

Amended by Chapter 173, 2025 General Session