LEGISLATIVE GENERAL COUNSEL
₵ Approved for Filing: S.C. Allred ₵
₵ 01-27-16 2:38 PM ₵

H.B. 225

CYBERCRIME AMENDMENTS

2016 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: David E. Lifferth

Senate Sponsor: Daniel W. Thatcher

LONG TITLE

General Description:

This bill modifies the Criminal Code regarding offenses committed by means of electronic or computer functions.

Highlighted Provisions:

This bill:

- defines critical infrastructure regarding computer crimes and creates the offense of interfering electronically or by computer with critical infrastructure;
- defines a denial of service and provides a penalty for causing a denial of service;
- provides that reporting a false emergency situation involving violence or harm, and also reporting that the nonexistent emergency is at a specified location, is a criminal offense;
- modifies an element of computer crimes to include a person who acts Ĥ→ **[~~with~~]** **without** ←Ĥ authorization, Ĥ→ **, or whose acts exceed authorization** , **[~~but then~~]** **and who** ←Ĥ commits a crime;
- modifies the reporting procedure for computer crime offenses Ĥ→ **, including reporting by state agencies** ←Ĥ ; and
- modifies the offense of electronic communication harassment to include distribution of personal identifying information.

Money Appropriated in this Bill:

None

Other Special Clauses:

None

H.B. 225

Utah Code Sections Affected:

AMENDS:

76-6-702, as last amended by Laws of Utah 2005, Chapter 72

76-6-703, as last amended by Laws of Utah 2010, Chapter 193

76-6-705, as last amended by Laws of Utah 1993, Chapter 38

76-9-105, as last amended by Laws of Utah 2002, Chapter 166

76-9-201, as last amended by Laws of Utah 2009, Chapter 326

76-9-202, as last amended by Laws of Utah 2002, Chapter 166

Be it enacted by the Legislature of the state of Utah:

Section 1. Section **76-6-702** is amended to read:

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, or facilitates the transmission of 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; **Ĥ→ [~~or~~]**

(iii) network connected devices; or ←Ĥ

(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) "Critical infrastructure" means the same as that term is defined in Subsection 76-6-106(1).

(9) "Damage" means any of the following that result from a violation of this part:

(a) physical harm to or loss of real, personal, or commercial property; and

(b) economic losses incurred by the victim.

(10) "Denial of service attack" means an attack or intrusion that is intended to disrupt legitimate access to a network resource or system.

[~~(8)~~] (11) "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~~] or

(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)~~] (12) "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)~~] (13) "Security system" means a computer, computer system, network, **Ĥ→ network connected device, ←Ĥ** 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)~~] (14) "Services" include computer time, data manipulation, and storage functions.

[~~(12)~~] (15) "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)~~] (16) "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.

Section 2. Section **76-6-703** is amended to read:

76-6-703. Computer crimes and penalties.

(1) A person who **Ĥ→ [~~with or~~] , acting ←Ĥ** without authorization **Ĥ→ or whose acts exceed authorization, ←Ĥ** gains or attempts to gain access to any computer and unlawfully alters, damages, destroys, discloses, or modifies any computer, computer network, computer property, computer system, computer program, or computer data or software, and [~~thereby~~] as a result causes economic or property damage, or both, to another person or entity, 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 financial or property 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 when the 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 when the financial or property 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;

(d) a second degree felony when the financial or property 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 Ĥ→ **[~~intentionally or knowingly, and with or~~] , acting** ←Ĥ without authorization, Ĥ→ **or whose acts exceed authorization,** ←Ĥ interferes with or interrupts computer services to another authorized to receive the services is guilty of a class A misdemeanor.

(5) A person who by means of a computer, computer network, computer property, computer system, computer program, computer data or software Ĥ→ **[~~intentionally or knowingly~~] unlawfully** ←Ĥ interferes with or interrupts critical infrastructure is guilty of a Ĥ→ **[~~third degree felony~~] class A misdemeanor** ←Ĥ .

[~~(5)~~] (6) 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.

Section 3. Section **76-6-705** is amended to read:

76-6-705. Reporting violations.

Ĥ→ **(1)** ←Ĥ Every person, except [~~those~~] a person to whom a statutory or common law privilege applies, who has reason to believe that [~~the provisions~~] any provision of Section 76-6-703 [~~are~~] is being or [~~have~~] has been violated shall report the suspected violation to:

Ĥ→ **[~~(1)~~] (a)** ←Ĥ 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[~~.~~]; or

Ĥ→ **[~~(2)~~] (b)** ←Ĥ a state or local law enforcement agency Ĥ→ **.**

(2) Every state agency that has reason to believe that any provision of Section 76-6-703 is being or has been violated within the agency's computer system or network shall report the suspected violation to the Utah Department of Public Safety, State Bureau of Investigation. ←Ĥ

Section 4. Section **76-9-105** is amended to read:

76-9-105. Making a false alarm -- Penalties.

(1) A person is guilty of making a false alarm if [~~he~~] the person initiates or circulates a report or warning of any fire, impending bombing, or other crime or catastrophe, knowing that the report or warning is false or baseless and is likely to cause evacuation of any building, place of assembly, or facility of public transport, to cause public inconvenience or alarm or action of any sort by any official or volunteer agency organized to deal with emergencies.

(2) (a) Making a false alarm relating to a weapon of mass destruction as defined in Section 76-10-401 is a second degree felony.

(b) Making a false alarm that alleges an ongoing act or an imminent threat of an act that causes or threatens to cause bodily harm, serious bodily injury, or death against another person is a Ĥ→ **[~~third degree felony~~] class A misdemeanor** ←Ĥ .

[~~(b)~~] (c) Making a false alarm other than under Subsection (2)(a) or (b) is a class B misdemeanor.

(3) In addition to any other penalty authorized by law, a court shall order any person convicted of a felony violation of this section to reimburse any federal, state, or local unit of government, or any private business, organization, individual, or entity for all expenses and losses incurred in responding to the violation, unless the court states on the record the reasons why the court finds the reimbursement would be inappropriate.

(a) "Adult" means a person 18 years of age or older.

(b) "Electronic communication" means any communication by electronic, electro-mechanical, or electro-optical communication device for the transmission and reception of audio, image, or text but does not include broadcast transmissions or similar communications that are not targeted at any specific individual.

(c) "Electronic communication device" includes telephone, facsimile, electronic mail, [~~or~~] pager, computer, or any device capable of electronic communication.

(d) "Minor" means a person who is younger than 18 years of age.

Ĥ→ [~~(e) "Personal identifying information" means the same as that term is defined in Section 76-6-1102.~~] ←Ĥ

(2) A person is guilty of electronic communication harassment and subject to prosecution in the jurisdiction where the communication originated or was received if **Ĥ→ the person, or a party whom the person has encouraged to act in violation of this Subsection (2), acts ←Ĥ** with intent to **Ĥ→ [~~annoy,~~] ←Ĥ** alarm, intimidate, **Ĥ→ [~~offend,~~] ←Ĥ** abuse, threaten, harass, **Ĥ→ [~~frighten,~~] ←Ĥ** or disrupt the electronic communications of another **Ĥ→ [~~, the person~~] and ←Ĥ** :

(a) (i) makes repeated contact by means of electronic communications, whether or not a conversation ensues; or

(ii) after the recipient has requested or informed the person not to contact the recipient, and the person repeatedly or continuously:

(A) contacts the electronic communication device of the recipient; or

(B) causes an electronic communication device of the recipient to ring or to receive other notification of attempted contact by means of electronic communication;

(b) makes contact by means of electronic communication and insults, taunts, or challenges the recipient of the communication or any person at the receiving location in a manner likely to provoke a violent or disorderly response;

(c) makes contact by means of electronic communication and threatens to inflict injury, physical harm, or damage to any person or the property of any person; **Ĥ→ [ƭ] or [ʇ] ←Ĥ**

(d) causes disruption, jamming, or overload of an electronic communication system through excessive message traffic or other means utilizing an electronic communication device **Ĥ→ [ƭ] . [ʇ] [~~; or~~**

~~(e) electronically publishes, posts, or otherwise makes available personal identifying information in a public online site or forum.~~] ←Ĥ

(b) asks for or requests the use of a party line or a public pay telephone on the pretext that an emergency exists, knowing that no emergency exists; [~~or~~]

(c) reports an emergency or causes an emergency to be reported to any public, private, or volunteer entity whose purpose is to respond to fire, police, or medical emergencies, when the [~~actor~~] person knows the reported emergency does not exist[~~.~~]; or

(d) makes a false report to an emergency response service, including a law enforcement dispatcher or a 911 emergency response service, or intentionally aids, abets, or causes a third party to make the false report, and the false report:

(i) describes an ongoing emergency situation that as reported is causing or poses an imminent threat of causing serious bodily injury, serious physical injury, or death; and

(ii) states that the emergency situation is occurring at a specified location.

(3) (a) A violation of Subsection (2)(a) or (b) is a class C misdemeanor.

(b) A violation of Subsection (2)(c) is a class B misdemeanor, except as provided under Subsection (3)(c).

(c) A violation of Subsection (2)(c) is a second degree felony if the report is regarding a weapon of mass destruction, as defined in Section 76-10-401.

(d) A violation of Subsection (2)(d) **Ĥ→ [~~:~~**

~~(i) is a third degree felony; or~~

~~(ii) is a second degree felony if the emergency responders while acting in response to the report cause physical injury to any resident or other person at the reported location~~] is a class A misdemeanor ←Ĥ .

(4) (a) In addition to any other penalty authorized by law, a court shall order any person convicted of a violation of this section to reimburse:

(i) any federal, state, or local unit of government, or any private business, organization, individual, or entity for all expenses and losses incurred in responding to the violation[~~, unless~~]; and

(ii) any person injured under Subsection (3)(d)(ii) for costs for the treatment of any injury, including treatment for psychological injuries caused by the offense.

(b) The court may require that the defendant pay less than the reimbursements required under Subsection (4)(a) only if the court states on the record the reasons why the reimbursement would be inappropriate.