

**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 ~~H→~~ [with]

**without ←H**

authorization, ~~H→~~ , **or whose acts exceed authorization** , [but then] **and who ←H** commits a crime;

▶ modifies the reporting procedure for computer crime offenses ~~H→~~ , **including reporting**

**by state agencies ←H** ; 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



28 **Utah Code Sections Affected:**

29 AMENDS:

- 30 76-6-702, as last amended by Laws of Utah 2005, Chapter 72
- 31 76-6-703, as last amended by Laws of Utah 2010, Chapter 193
- 32 76-6-705, as last amended by Laws of Utah 1993, Chapter 38
- 33 76-9-105, as last amended by Laws of Utah 2002, Chapter 166
- 34 76-9-201, as last amended by Laws of Utah 2009, Chapter 326
- 35 76-9-202, as last amended by Laws of Utah 2002, Chapter 166



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

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

39 **76-6-702. Definitions.**

40 As used in this part:

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

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

48 (3) "Computer" means any electronic device or communication facility that stores,  
49 ~~retrieves,~~ processes, ~~or~~ transmits, or facilitates the transmission of data.

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

52 (5) "Computer network" means:

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

54 (i) computers; or

55 (ii) computers and remote terminals; ~~H~~→ [or]

55a **(iii) network connected devices; or ←H**

56 (b) the interconnection by wireless technology between:

57 (i) computers; or

58 (ii) computers and remote terminals.

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

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

66 (8) "Critical infrastructure" means the same as that term is defined in Subsection  
67 76-6-106(1).

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

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

70 (b) economic losses incurred by the victim.

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

73 [~~(8)~~] (11) "Information" does not include information obtained:

74 (a) through use of:

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

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

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

79 [~~(9)~~] (12) "License or entitlement" includes:

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

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

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

83 (d) membership and standing in organizations and religious institutions;

84 (e) certification as a peace officer;

85 (f) credit reports; and

86 (g) another record or datum upon which a person may be reasonably expected to rely in  
87 making decisions that will have a direct benefit or detriment to another.

88 [~~(10)~~] (13) "Security system" means a computer, computer system, network, ~~H~~→ **network**  
88a **connected device**, ←~~H~~ or

89 computer property that has some form of access control technology implemented, such as

90 encryption, password protection, other forced authentication, or access control designed to keep  
91 out unauthorized persons.

92 ~~[(11)]~~ (14) "Services" include computer time, data manipulation, and storage functions.

93 ~~[(12)]~~ (15) "Financial instrument" includes any check, draft, money order, certificate of  
94 deposit, letter of credit, bill of exchange, electronic fund transfer, automated clearing house  
95 transaction, credit card, or marketable security.

96 ~~[(13)]~~ (16) "Software" or "program" means a series of instructions or statements in a  
97 form acceptable to a computer, relating to the operations of the computer, or permitting the  
98 functioning of a computer system in a manner designed to provide results including system  
99 control programs, application programs, or copies of any of them.

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

101 **76-6-703. Computer crimes and penalties.**

102 (1) A person who ~~H→~~ **[with or]**, **acting ←H** without authorization ~~H→~~ **or whose acts**  
102a **exceed authorization,** ~~←H~~ gains or attempts to gain access to any  
103 computer and unlawfully alters, damages, destroys, discloses, or modifies any computer,  
104 computer network, computer property, computer system, computer program, or computer data  
105 or software, and ~~[thereby]~~ as a result causes economic or property damage, or both, to another  
106 person or entity, or obtains money, property, information, or a benefit for any person without  
107 legal right, is guilty of:

108 (a) a class B misdemeanor when:

109 (i) the financial or property damage caused or the value of the money, property, or  
110 benefit obtained or sought to be obtained is less than \$500; or

111 (ii) the information obtained is not confidential;

112 (b) a class A misdemeanor when the damage caused or the value of the money,  
113 property, or benefit obtained or sought to be obtained is or exceeds \$500 but is less than  
114 \$1,500;

115 (c) a third degree felony when the financial or property damage caused or the value of  
116 the money, property, or benefit obtained or sought to be obtained is or exceeds \$1,500 but is  
117 less than \$5,000;

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

120 (e) a third degree felony when:

- 121 (i) the property or benefit obtained or sought to be obtained is a license or entitlement;  
 122 (ii) the damage is to the license or entitlement of another person; or  
 123 (iii) the information obtained is confidential; or  
 124 (iv) in gaining access the person breaches or breaks through a security system.

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

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

134 (3) A person who uses or knowingly allows another person to use any computer,  
 135 computer network, computer property, or computer system, program, or software to devise or  
 136 execute any artifice or scheme to defraud or to obtain money, property, services, or other things  
 137 of value by false pretenses, promises, or representations, is guilty of an offense based on the  
 138 value of the money, property, services, or things of value, in the degree set forth in Subsection  
 139 76-10-1801(1).

140 (4) A person who ~~H→ [intentionally or knowingly, and with or]~~ , acting ~~←H~~ without  
 140a authorization, ~~H→ or whose acts exceed authorization,~~ ~~←H~~  
 141 interferes with or interrupts computer services to another authorized to receive the services is  
 142 guilty of a class A misdemeanor.

143 (5) A person who by means of a computer, computer network, computer property,  
 144 computer system, computer program, computer data or software ~~H→ [intentionally or knowingly]~~  
 144a ~~unlawfully~~ ~~←H~~  
 145 ~~interferes with or interrupts critical infrastructure is guilty of a~~ ~~H→ [third degree felony]~~ ~~class A~~  
 145a ~~misdemeanor~~ ~~←H~~ .

146 [(5)] (6) It is an affirmative defense to Subsections (1) and (2) that a person obtained  
 147 access or attempted to obtain access in response to, and for the purpose of protecting against or  
 148 investigating, a prior attempted or successful breach of security of a computer, computer  
 149 network, computer property, computer system whose security the person is authorized or  
 150 entitled to protect, and the access attempted or obtained was no greater than reasonably  
 151 necessary for that purpose.

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

153 **76-6-705. Reporting violations.**

154 ~~H~~→ (1) ~~←H~~ Every person, except ~~[those]~~ a person to whom a statutory or common law  
154a privilege

155 applies, who has reason to believe that ~~[the provisions]~~ any provision of Section 76-6-703 ~~[are]~~  
156 is being or ~~[have]~~ has been violated shall report the suspected violation to:

157 ~~H~~→ ~~[(1)]~~ (a) ~~←H~~ the attorney general~~;~~ or county attorney, or, if within a prosecution  
157a district, the

158 district attorney of the county or prosecution district in which part or all of the violations  
159 occurred~~;~~; or

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

160a **(2) Every state agency that has reason to believe that any provision of Section 76-6-703**

160b **is being or has been violated within the agency's computer system or network shall**

160c **report the suspected violation to the Utah Department of Public Safety, State Bureau of**

160d **Investigation.** ~~←H~~

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

162 **76-9-105. Making a false alarm -- Penalties.**

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

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

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

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

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

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

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

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

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

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

193 (2) A person is guilty of electronic communication harassment and subject to  
194 prosecution in the jurisdiction where the communication originated or was received if ~~H→~~ the  
194a person, or a party whom the person has encouraged to act in violation of this Subsection (2),  
194b acts ←H with

195 intent to ~~H→~~ [annoy;] ←H alarm, intimidate, ~~H→~~ [offend;] ←H abuse, threaten, harass,  
195a ~~H→~~ [frighten;] ←H or disrupt the  
196 electronic communications of another ~~H→~~ [~~the person~~] and ←H :

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

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

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

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

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

207 (c) makes contact by means of electronic communication and threatens to inflict injury,  
208 physical harm, or damage to any person or the property of any person; ~~H→~~ [f] or [j] ←H

209 (d) causes disruption, jamming, or overload of an electronic communication system  
210 through excessive message traffic or other means utilizing an electronic communication  
211 device ~~H→~~ [f] . [j] [~~or~~

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

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

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

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

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

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

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

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

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

261 (d) A violation of Subsection (2)(d) ~~H~~→ [:

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

263 ~~—— (ii) is a second degree felony if the emergency responders while acting in response to~~

264 ~~the report cause physical injury to any resident or other person at the reported location] is a class A~~  
264a ~~misdemeanor~~ ←H .

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

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

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

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