

COMPUTER ABUSE AND DATA RECOVERY ACT

2016 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Rebecca Chavez-Houck

Senate Sponsor: Todd Weiler

6	Cosponsors:	Stephen G. Handy	V. Lowry Snow
7	Patrice M. Arent	Lynn N. Hemingway	Keven J. Stratton
8	Scott H. Chew	Ken Ivory	Earl D. Tanner
9	Kay J. Christofferson	Brian S. King	
10	Keith Grover	Kraig Powell	

LONG TITLE

General Description:

This bill enacts provisions related to unauthorized access to information technology.

Highlighted Provisions:

This bill:

provides civil penalties for an individual who, without authorization from a protected computer's owner:

- obtains information from the protected computer;
- causes the transmission of a program, code, or command to the protected computer; or

traffics in a technological access barrier that could be used to access the protected computer;

defines terms; and

provides that the prevailing party in a civil action under this act is entitled to attorney fees.

Money Appropriated in this Bill:

None

29 **Other Special Clauses:**

30 None

31 **Utah Code Sections Affected:**

32 ENACTS:

33 **63D-3-101**, Utah Code Annotated 1953

34 **63D-3-102**, Utah Code Annotated 1953

35 **63D-3-103**, Utah Code Annotated 1953

36 **63D-3-104**, Utah Code Annotated 1953

37 **63D-3-105**, Utah Code Annotated 1953

38 **63D-3-106**, Utah Code Annotated 1953



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

41 Section 1. Section **63D-3-101** is enacted to read:

42 **CHAPTER 3. UNAUTHORIZED ACCESS TO INFORMATION TECHNOLOGY**

43 **Part 1. Computer Abuse and Data Recovery Act**

44 **63D-3-101. Title.**

45 (1) This chapter is known as "Unauthorized Access to Information Technology."

46 (2) This part is known as "Computer Abuse and Data Recovery Act."

47 Section 2. Section **63D-3-102** is enacted to read:

48 **63D-3-102. Definitions.**

49 As used in this part, the term:

50 (1) "Authorized user" means, for a protected computer:

51 (a) the protected computer's owner; or

52 (b) an individual who has permission to access the protected computer under Section

53 [63D-3-103](#).

54 (2) (a) "Computer" means an electronic, magnetic, optical, electrochemical, or other  
55 high-speed data processing device that performs logical, arithmetic, or storage functions.

56 (b) "Computer" includes any data storage device, data storage facility, or

57 communications facility that is directly related to or that operates in conjunction with the  
58 device described in Subsection (2)(a).

59 (3) (a) "Damage" means, for a protected computer's owner, the cost associated with an  
60 individual's unauthorized access to information stored on a protected computer.

61 (b) "Damage" includes:

62 (i) the cost of repairing or restoring a protected computer;

63 (ii) economic damages;

64 (iii) consequential damages, including interruption of service; and

65 (iv) profit by the individual from the unauthorized access to the protected computer.

66 (4) "Harm" means any impairment to the integrity, access, or availability of:

67 (a) data;

68 (b) a program;

69 (c) a system; or

70 (d) information.

71 (5) "Owner" means a person who:

72 (a) owns or leases a protected computer; or

73 (b) owns the information stored in a protected computer.

74 (6) (a) "Protected computer" means a computer that:

75 (i) is used in connection with the operation of a business, state government entity, or  
76 political subdivision; and

77 (ii) requires a technological access barrier for an individual to access the computer.

78 (b) "Protected computer" does not include a computer that an individual can access  
79 using a technological access barrier that does not, to a reasonable degree of security, effectively  
80 control access to the information stored in the computer.

81 (7) "Technological access barrier" means a password, security code, token, key fob,  
82 access device, or other digital security measure.

83 (8) "Traffic" means to sell, purchase, or deliver.

84 (9) "Unauthorized user" means an individual who, for a protected computer:

- 85 (a) is not an authorized user of the protected computer; and
- 86 (b) accesses the protected computer by:
- 87 (i) obtaining, without an authorized user's permission, the authorized user's
- 88 technological access barrier; or
- 89 (ii) circumventing, without the permission of the protected computer's owner, a
- 90 technological access barrier on the protected computer.

91 Section 3. Section **63D-3-103** is enacted to read:

92 **63D-3-103. Permission to access a protected computer -- Revocation.**

93 (1) Subject to Subsections (2) and (3), an individual has permission to access a

94 protected computer if:

- 95 (a) the individual is a director, officer, employee, agent, or contractor of the protected
- 96 computer's owner; and
- 97 (b) the protected computer's owner gave the individual express permission to access
- 98 the protected computer through a technological access barrier.

99 (2) If a protected computer's owner gives an individual permission to access the

100 protected computer, the permission is valid only to the extent or for the specific purpose the

101 protected computer's owner authorizes.

102 (3) An individual's permission to access a protected computer is revoked if:

- 103 (a) the protected computer's owner expressly revokes the individual's permission to
- 104 access the protected computer; or
- 105 (b) the individual ceases to be a director, officer, employee, agent, or contractor of the
- 106 protected computer's owner.

107 Section 4. Section **63D-3-104** is enacted to read:

108 **63D-3-104. Prohibited acts.**

109 (1) An unauthorized user of a protected computer may not, knowingly and with intent

110 to cause harm or damage:

- 111 (a) obtain information from the protected computer and, as a result, cause harm or
- 112 damage;

113 (b) cause the transmission of a program, code, or command to the protected computer,  
114 and, as a result of the transmission, cause harm or loss; or

115 (c) traffic in any technological access barrier that an unauthorized user could use to  
116 access the protected computer.

117 (2) An individual who violates Subsection (1) is liable to a protected computer's owner  
118 in a civil action for the remedies described in Section [63D-3-105](#).

119 Section 5. Section **63D-3-105** is enacted to read:

120 **63D-3-105. Remedies.**

121 (1) A person who brings a civil action against an individual for a violation of Section  
122 [63D-3-104](#) may:

123 (a) recover actual damages, including the person's:

124 (i) lost profits;

125 (ii) economic damages; and

126 (iii) reasonable cost of remediation efforts related to the violation;

127 (b) recover consequential damages, including for interruption of service;

128 (c) recover, from the individual, the individual's profit obtained through trafficking in  
129 anything obtained by the individual through the violation;

130 (d) obtain injunctive or other equitable relief to prevent a future violation of Section  
131 [63D-3-104](#); and

132 (e) recover anything the individual obtained through the violation, including:

133 (i) misappropriated information or code;

134 (ii) a misappropriated program; and

135 (iii) any copies of the information, code, or program described in Subsections (1)(e)(i)  
136 and (1)(e)(ii).

137 (2) A court shall award reasonable attorney fees to the prevailing party in any action  
138 arising under this part.

139 (3) The remedies available for a violation of Section [63D-3-104](#) are in addition to  
140 remedies otherwise available for the same conduct under federal or state law.

141           (4) A person may not file a civil action under Section 63D-3-104 later than three years  
142 after the day on which:  
143           (a) the violation occurred; or  
144           (b) (i) the person discovers the violation; or  
145           (ii) the person should have discovered the violation if the person acted with reasonable  
146 diligence to discover the violation.

147           Section 6. Section **63D-3-106** is enacted to read:

148           **63D-3-106. Exclusions.**

149           (1) This section does not prohibit a lawfully authorized investigative, protective, or  
150 intelligence activity of a law enforcement agency, regulatory agency, or political subdivision of  
151 this state, another state, the United States, or a foreign country.

152           (2) This part does not apply to a provider of:

153           (a) an interactive computer service as defined in 47 U.S.C. Sec. 230(f); or

154           (b) an information service as defined in 47 U.S.C. Sec. 153.