

**House Study Bill 645 - Introduced**

HOUSE FILE \_\_\_\_\_

BY (PROPOSED COMMITTEE ON  
INFORMATION TECHNOLOGY BILL  
BY CHAIRPERSON LOHSE)

**A BILL FOR**

- 1 An Act relating to ransomware and providing penalties.
- 2 BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

1 Section 1. Section 715.2, Code 2022, is amended to read as  
2 follows:

3 **715.2 Title.**

4 This chapter shall be known and may be cited as the "*Computer*  
5 *Spyware, Malware, and Ransomware Protection Act*".

6 Sec. 2. Section 715.3, Code 2022, is amended by adding the  
7 following new subsections:

8 NEW SUBSECTION. 1A. "*Computer control language*" means  
9 ordered statements that direct a computer to perform specific  
10 functions.

11 NEW SUBSECTION. 1B. "*Computer database*" means a  
12 representation of information, knowledge, facts, concepts, or  
13 instructions that is intended for use in a computer, computer  
14 system, or computer network that is being prepared or has been  
15 prepared in a formalized manner, or is being produced or has  
16 been produced by a computer, computer system, or computer  
17 network.

18 NEW SUBSECTION. 9A. "*Ransomware*" means a computer or data  
19 contaminant, encryption, or lock that is placed or introduced  
20 without authorization into a computer, computer network, or  
21 computer system that restricts access by an authorized person  
22 to a computer, computer data, a computer system, or a computer  
23 network in a manner that results in the person responsible for  
24 the placement or introduction of the contaminant, encryption,  
25 or lock making a demand for payment of money or other  
26 consideration to remove the contaminant, encryption, or lock.

27 Sec. 3. Section 715.5, subsection 2, Code 2022, is amended  
28 to read as follows:

29 2. Using intentionally deceptive means to cause the  
30 execution of a computer software component with the intent of  
31 causing an owner or operator to use such component in a manner  
32 that violates any other provision of [this chapter subchapter](#).

33 Sec. 4. Section 715.6, Code 2022, is amended to read as  
34 follows:

35 **715.6 Exceptions.**

1 Sections 715.4 and 715.5 shall not apply to the monitoring  
2 of, or interaction with, an owner's or an operator's internet  
3 or other network connection, service, or computer, by a  
4 telecommunications carrier, cable operator, computer hardware  
5 or software provider, or provider of information service or  
6 interactive computer service for network or computer security  
7 purposes, diagnostics, technical support, maintenance, repair,  
8 authorized updates of computer software or system firmware,  
9 authorized remote system management, or detection, criminal  
10 investigation, or prevention of the use of or fraudulent  
11 or other illegal activities prohibited in this ~~chapter~~  
12 subchapter in connection with a network, service, or computer  
13 software, including scanning for and removing computer software  
14 prescribed under this chapter subchapter. Nothing in this  
15 ~~chapter subchapter~~ shall limit the rights of providers of wire  
16 and electronic communications under 18 U.S.C. §2511.

17 Sec. 5. Section 715.7, Code 2022, is amended to read as  
18 follows:

19 **715.7 Criminal penalties.**

20 1. A person who commits an unlawful act under this ~~chapter~~  
21 subchapter is guilty of an aggravated misdemeanor.

22 2. A person who commits an unlawful act under this ~~chapter~~  
23 subchapter and who causes pecuniary losses exceeding one  
24 thousand dollars to a victim of the unlawful act is guilty of a  
25 class "D" felony.

26 Sec. 6. Section 715.8, unnumbered paragraph 1, Code 2022,  
27 is amended to read as follows:

28 For the purpose of determining proper venue, a violation  
29 of this chapter subchapter shall be considered to have been  
30 committed in any county in which any of the following apply:

31 Sec. 7. NEW SECTION. **715.9 Ransomware prohibition.**

32 1. A person shall not intentionally, willfully, and without  
33 authorization do any of the following:

34 a. Access, attempt to access, cause to be accessed, or  
35 exceed the person's authorized access to all or a part of a

1 computer network, computer control language, computer, computer  
2 software, computer system, or computer database.

3 *b.* Copy, attempt to copy, possess, or attempt to possess  
4 the contents of all or part of a computer database accessed in  
5 violation of paragraph "a".

6 2. A person shall not commit an act prohibited in subsection  
7 1 with the intent to do any of the following:

8 *a.* Cause the malfunction or interruption of the operation  
9 of all or any part of a computer, computer network, computer  
10 control language, computer software, computer system, computer  
11 service, or computer data.

12 *b.* Alter, damage, or destroy all or any part of data or a  
13 computer program stored, maintained, or produced by a computer,  
14 computer network, computer software, computer system, computer  
15 service, or computer database.

16 3. A person shall not intentionally, willfully, and without  
17 authorization do any of the following:

18 *a.* Possess, identify, or attempt to identify a valid  
19 computer access code.

20 *b.* Publicize or distribute a valid computer access code to  
21 an unauthorized person.

22 4. A person shall not commit an act prohibited under this  
23 section with the intent to interrupt or impair the functioning  
24 of any of the following:

25 *a.* The state.

26 *b.* A service, device, or system related to the production,  
27 transmission, delivery, or storage of electricity or natural  
28 gas in the state that is owned, operated, or controlled by a  
29 person other than a public utility as defined in chapter 476.

30 *c.* A service provided in the state by a public utility as  
31 defined in chapter 476.

32 *d.* A hospital or health care facility as defined in section  
33 135C.1.

34 *e.* A public elementary or secondary school, community  
35 college, or area education agency under the supervision of the

1 department of education.

2 5. This section shall not apply to the use of ransomware for  
3 research purposes by a person who has a bona fide scientific,  
4 educational, governmental, testing, news, or other similar  
5 justification for possessing ransomware. However, a person  
6 shall not knowingly possess ransomware with the intent to  
7 use the ransomware for the purpose of introduction into the  
8 computer, computer network, or computer system of another  
9 person without the authorization of the other person.

10 6. A person who has suffered a specific and direct injury  
11 because of a violation of this section may bring a civil action  
12 in a court of competent jurisdiction.

13 a. In an action under this subsection, the court may award  
14 actual damages, reasonable attorney fees, and court costs.

15 b. A conviction for an offense under this section is not a  
16 prerequisite for the filing of a civil action.

17 Sec. 8. NEW SECTION. 715.10 **Criminal penalties.**

18 1. A person who commits an unlawful act under this  
19 subchapter and who causes pecuniary losses involving less than  
20 ten thousand dollars to a victim of the unlawful act is guilty  
21 of an aggravated misdemeanor.

22 2. A person who commits an unlawful act under this  
23 subchapter and who causes pecuniary losses involving at least  
24 ten thousand dollars but less than fifty thousand dollars to a  
25 victim of the unlawful act is guilty of a class "D" felony.

26 3. A person who commits an unlawful act under this  
27 subchapter and who causes pecuniary losses involving at least  
28 fifty thousand dollars to a victim of the unlawful act is  
29 guilty of a class "C" felony.

30 Sec. 9. NEW SECTION. 715.11 **Venue.**

31 For the purpose of determining proper venue, a violation of  
32 this subchapter shall be considered to have been committed in  
33 any county in which any of the following apply:

34 1. Where the defendant performed the unlawful act.

35 2. Where the defendant resides.

1 3. Where the accessed computer is located.

2 Sec. 10. CODE EDITOR DIRECTIVE. The Code editor shall  
3 divide chapter 715 into subchapters and shall designate  
4 sections 715.1 through 715.8, including sections amended in  
5 this Act, as subchapter I entitled "COMPUTER SPYWARE AND  
6 MALWARE", and sections 715.9 through 715.11, as enacted in this  
7 Act, as subchapter II entitled "RANSOMWARE".

8 EXPLANATION

9 The inclusion of this explanation does not constitute agreement with  
10 the explanation's substance by the members of the general assembly.

11 This bill relates to ransomware.

12 The bill defines "ransomware" as a computer or data  
13 contaminant, encryption, or lock that is placed or introduced  
14 without authorization into a computer, computer network, or a  
15 computer system that restricts access by an authorized person  
16 to a computer, computer data, a computer network, or a computer  
17 system in a manner that results in the person responsible for  
18 the placement or introduction of the contaminant, encryption,  
19 or lock making a demand for payment of money or other  
20 consideration to remove the contaminant, encryption, or lock.

21 The bill provides that a person shall not do any of  
22 the following with the intent to cause the malfunction or  
23 interruption of the operation of, or alter, damage, or destroy,  
24 all or any part of a computer, computer network, computer  
25 control language, computer software, computer system, computer  
26 service, or computer data: intentionally, willfully, and  
27 without authorization access, attempt to access, cause to be  
28 accessed, or exceed the person's authorized access to all  
29 or a part of a computer network, computer control language,  
30 computer, computer software, computer system, or computer  
31 database; or copy, attempt to copy, possess, or attempt to  
32 possess the contents of all or part of a computer database.

33 The bill provides that a person shall not intentionally,  
34 willfully, and without authorization possess, identify,  
35 or attempt to identify a valid access code or publicize or

1 distribute a valid access code to an unauthorized person.

2 The bill provides that a person shall not commit a prohibited  
3 act with the intent to interrupt or impair the functioning of  
4 the state government; a service, device, or system related  
5 to the production, transmission, delivery, or storage of  
6 electricity or natural gas in the state that is owned,  
7 operated, or controlled by a person other than a public utility  
8 as defined in Code chapter 476; a service provided in the state  
9 by a public utility as defined in Code chapter 476; a hospital  
10 or health care facility; or a public elementary or secondary  
11 school, community college, or area education agency under the  
12 supervision of the department of education.

13 The bill does not apply to the use of ransomware for  
14 research purposes by a person who has a bona fide scientific,  
15 educational, governmental, testing, news, or other similar  
16 justification for possessing ransomware. However, a person  
17 shall not knowingly possess ransomware with the intent to  
18 use the ransomware for the purpose of introduction into the  
19 computer, computer network, or computer system of another  
20 person without the authorization of the other person.

21 The bill provides that a person who has suffered a specific  
22 and direct injury because of a violation of the bill may bring  
23 a civil action in a court of competent jurisdiction, and the  
24 court may award actual damages, reasonable attorney fees, and  
25 court costs. A conviction for an offense under the bill is not  
26 a prerequisite for the filing of a civil action.

27 The bill provides that a person who commits a violation  
28 of the bill and who causes pecuniary losses involving less  
29 than \$10,000 to a victim of the unlawful act is guilty of an  
30 aggravated misdemeanor. A person who commits a violation of  
31 the bill and who causes pecuniary losses involving at least  
32 \$10,000 but less than \$50,000 to a victim of the unlawful  
33 act is guilty of a class "D" felony. A person who commits a  
34 violation of the bill and who causes pecuniary losses involving  
35 at least \$50,000 to a victim of the unlawful act is guilty of a

1 class "C" felony.

2 An aggravated misdemeanor is punishable by confinement for  
3 no more than two years and a fine of at least \$855 but not more  
4 than \$8,540. A class "D" felony is punishable by confinement  
5 for no more than five years and a fine of at least \$1,025 but  
6 not more than \$10,245. A class "C" felony is punishable by  
7 confinement for no more than 10 years and a fine of at least  
8 \$1,370 but not more than \$13,660.

9 The bill provides that for the purpose of determining  
10 venue, a violation of the bill shall be considered to have  
11 been committed in any county where the defendant performed  
12 the unlawful act, where the defendant resides, or where the  
13 accessed computer is located.