

## **IC 24-4.8-2**

### **Chapter 2. Prohibited Conduct**

#### **IC 24-4.8-2-1**

##### **Application**

Sec. 1. This chapter does not apply to a person who monitors or interacts with an owner or operator's Internet connection, Internet service, network connection, or computer if the person is a telecommunications carrier, cable operator, computer hardware or software provider, or other computer service provider who monitors or interacts with an owner or operator's Internet connection, Internet service, network connection, or computer for one (1) or more of the following purposes:

- (1) Network security.
- (2) Computer security.
- (3) Diagnosis.
- (4) Technical support.
- (5) Maintenance.
- (6) Repair.
- (7) Authorized updates of software or system firmware.
- (8) Authorized remote system management.
- (9) Detection or prevention of the unauthorized, illegal, or fraudulent use of a network, service, or computer software, including scanning for and removing computer software that facilitates a violation of this chapter.

*As added by P.L.115-2005, SEC.1.*

#### **IC 24-4.8-2-2**

##### **Prohibited conduct by owners or operators of computers**

Sec. 2. A person who is not the owner or operator of the computer may not knowingly or intentionally:

- (1) transmit computer software to the computer; and
- (2) by means of the computer software transmitted under subdivision (1), do any of the following:
  - (A) Use intentionally deceptive means to modify computer settings that control:
    - (i) the page that appears when an owner or operator opens an Internet browser or similar computer software used to access and navigate the Internet;
    - (ii) the Internet service provider, search engine, or web proxy that an owner or operator uses to access or search the Internet; or
    - (iii) the owner or operator's list of bookmarks used to access web pages.
  - (B) Use intentionally deceptive means to collect personally identifying information:
    - (i) through the use of computer software that records a keystroke made by an owner or operator and transfers that

- information from the computer to another person; or
- (ii) in a manner that correlates the personally identifying information with data respecting all or substantially all of the web sites visited by the owner or operator of the computer, not including a web site operated by the person collecting the personally identifying information.
- (C) Extract from the hard drive of an owner or operator's computer:
- (i) a credit card number, debit card number, bank account number, or any password or access code associated with these numbers;
  - (ii) a Social Security number, tax identification number, driver's license number, passport number, or any other government issued identification number; or
  - (iii) the account balance or overdraft history of a person in a form that identifies the person.
- (D) Use intentionally deceptive means to prevent reasonable efforts by an owner or operator to block or disable the installation or execution of computer software.
- (E) Knowingly or intentionally misrepresent that computer software will be uninstalled or disabled by an owner or operator's action.
- (F) Use intentionally deceptive means to remove, disable, or otherwise make inoperative security, antispyware, or antivirus computer software installed on the computer.
- (G) Take control of another person's computer with the intent to cause damage to the computer or cause the owner or operator to incur a financial charge for a service that the owner or operator has not authorized by:
- (i) accessing or using the computer's modem or Internet service; or
  - (ii) without the authorization of the owner or operator, opening multiple, sequential, standalone advertisements in the owner or operator's Internet browser that a reasonable computer user cannot close without turning off the computer or closing the browser.
- (H) Modify:
- (i) computer settings that protect information about a person with the intent of obtaining personally identifying information without the permission of the owner or operator; or
  - (ii) security settings with the intent to cause damage to a computer.
- (I) Prevent reasonable efforts by an owner or operator to block or disable the installation or execution of computer software by:
- (i) presenting an owner or operator with an option to

decline installation of computer software knowing that the computer software will be installed even if the owner or operator attempts to decline installation; or  
(ii) falsely representing that computer software has been disabled.

*As added by P.L.115-2005, SEC.1.*

### **IC 24-4.8-2-3**

#### **Prohibited conduct by persons who are not owners or operators of computers**

Sec. 3. A person who is not the owner or operator may not knowingly or intentionally do any of the following:

(1) Induce the owner or operator to install computer software on the owner or operator's computer by knowingly or intentionally misrepresenting the extent to which installing the computer software is necessary for:

(A) computer security;

(B) computer privacy; or

(C) opening, viewing, or playing a particular type of content.

(2) Use intentionally deceptive means to execute or cause the execution of computer software with the intent to cause the owner or operator to use the computer software in a manner that violates subdivision (1).

*As added by P.L.115-2005, SEC.1.*