A.R.S. § 18-502

Current through chapter 1 of the 56th Legislature's 2nd Regular session (2024), including all legislation enacted through March 1, 2024

LexisNexis® Arizona Annotated Revised Statutes > Title 18 Information Technology (Chs. 1 — 6) > Chapter 5 Network Security (Arts. 1 — 4) > Article 1. Computer Spyware (§§ 18-501 — 18-504)

18-502. Prohibited activities; applicability

A. It is unlawful for any person who is not an owner or operator of a computer to transmit computer software to a computer, with actual knowledge or with conscious avoidance of actual knowledge, and to use the software to do any of the following:

1. Modify, through intentionally deceptive means, settings that control any of the following:

(a) The page that appears when an owner or operator of a computer launches an internet browser or similar computer software used to access and navigate the internet.

(b) The default provider or web proxy that an owner or operator of a computer uses to access or search the internet.

(c) An owner's or operator's list of bookmarks used to access web pages.

2. Collect, through intentionally deceptive means, personally identifiable information:

(a) Through the use of a keystroke logging function that records all keystrokes made by an authorized user who uses the computer and transfers that information from the computer to another person.

(b) In a manner that correlates the information with data respecting all or substantially all of the websites visited by an owner or operator of the computer, other than websites operated by the person collecting the information.

(c) With respect only to information described in section 18-501, paragraph 9, by extracting such information from the hard drive of an owner's or operator's computer.

3. Prevent, through intentionally deceptive means, an owner's or operator's reasonable efforts to block the installation or execution of, or to disable, computer software by causing software that an owner or operator of the computer has properly removed or disabled automatically to reinstall or reactivate on the computer.

4. Intentionally misrepresent that computer software will be uninstalled or disabled by an owner's or operator's action.

5. Through intentionally deceptive means, remove, disable or render inoperative security, antispyware or antivirus computer software installed on the computer.

6. Take control of the computer by:

(a) Accessing or using the modem or internet service for the computer for the purpose of causing damage to the computer or causing an owner or operator to incur financial charges for a service that the owner or operator of the computer has not authorized.

(b) Opening multiple, sequential, stand-alone advertisements in an owner's or operator's internet browser without the authorization of the owner or operator that a reasonable computer user cannot close without turning off the computer or closing the internet browser.

7. Modify any of the following settings related to the computer's access to, or use of, the internet:

(a) Settings that protect information about an owner or operator of the computer for the purpose of stealing personally identifiable information of the owner or operator.

(b) Security settings for the purpose of causing damage to a computer.

8. Prevent an owner's or operator's reasonable efforts to block the installation of, or to disable, computer software, by doing either of the following:

(a) Presenting the owner or operator with an option to decline installation of computer software with knowledge that, if the option is selected, the installation nevertheless proceeds.

(b) Falsely representing that computer software has been disabled.

B. It is unlawful for any person who is not an owner or operator of a computer to do either of the following with regard to the computer:

1. Induce an owner or operator to install a computer software component on the computer by intentionally misrepresenting the extent to which installing the software is necessary for security or privacy reasons or in order to open, view or play a particular type of content.

2. Deceptively cause the execution on the computer of a computer software component with the intent of causing an owner or operator to use the component in a manner that violates any other provision of this section.

C. This section does not apply to any monitoring of, or interaction with, a subscriber's internet or other network connection or service, or a computer, by a telecommunications carrier, cable operator, video service provider, computer hardware or software provider or provider of information service or interactive computer service for network or computer security purposes, diagnostics, technical support, maintenance, repair, authorized updates of software or system firmware, authorized remote system management or detection or prevention of the unauthorized use of or fraudulent or other illegal activities in connection with a network, service or computer software, including scanning for and removing software prescribed under this article.

History

Recent legislative history: Transferred and renumbered as A.R.S. § 18-502, effective August 6, 2016, by Laws 2016, 2nd Reg. Sess., Ch. 80, § 3(E); renumbered from § 44-7302 by 2016 2nd Reg. Sess. Ch. 80, § 3(E), effective August 6, 2016; 2019 1st Reg. Sess. Ch. 163, § 10, effective August 27, 2019.

End of Document