

## Cal Bus & Prof Code § 22947.3

Deering's California Codes are current through the 2024 Regular Session Ch 1

*Deering's California Codes Annotated > BUSINESS & PROFESSIONS CODE (§§ 1 — 30047) > Division 8  
Special Business Regulations (Chs. 1 — 40) > Chapter 32 Consumer Protection Against Computer Spyware Act  
(§§ 22947 — 22947.6)*

### **§ 22947.3. Taking control of computer; Modifying other settings; Means of preventing user's efforts to block or disable software; Exceptions**

---

A person or entity that is not an authorized user, as defined in Section 22947.1, shall not, with actual knowledge, with conscious avoidance of actual knowledge, or willfully, cause computer software to be copied onto the computer of a consumer in this state and use the software to do any of the following:

- (a) Take control of the consumer's computer by doing any of the following:
  - (1) Transmitting or relaying commercial electronic mail or a computer virus from the consumer's computer, where the transmission or relaying is initiated by a person other than the authorized user and without the authorization of an authorized user.
  - (2) Accessing or using the consumer's modem or Internet service for the purpose of causing damage to the consumer's computer or of causing an authorized user to incur financial charges for a service that is not authorized by an authorized user.
  - (3) Using the consumer's computer as part of an activity performed by a group of computers for the purpose of causing damage to another computer, including, but not limited to, launching a denial of service attack.
  - (4) Opening multiple, sequential, stand-alone advertisements in the consumer's Internet browser without the authorization of an authorized user and with knowledge that a reasonable computer user cannot close the advertisements without turning off the computer or closing the consumer's Internet browser.
- (b) Modify any of the following settings related to the computer's access to, or use of, the Internet:
  - (1) An authorized user's security or other settings that protect information about the authorized user for the purpose of stealing personal information of an authorized user.
  - (2) The security settings of the computer for the purpose of causing damage to one or more computers.
- (c) Prevent, without the authorization of an authorized user, an authorized user's reasonable efforts to block the installation of, or to disable, software, by doing any of the following:

(1) Presenting the authorized user with an option to decline installation of software with knowledge that, when the option is selected by the authorized user, the installation nevertheless proceeds.

(2) Falsely representing that software has been disabled.

(d) Nothing in this section shall apply to any monitoring of, or interaction with, a subscriber's Internet or other network connection or service, or a protected computer, by a telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service or interactive computer service for network or computer security purposes, diagnostics, technical support, 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 proscribed under this chapter.

## History

---

Added Stats 2004 ch 843 § 2 (SB 1436).

Deering's California Codes Annotated  
Copyright © 2024 All rights reserved.