A.C.A. § 4-111-103

Current through all legislation of the 2023 Regular Session and the 2023 First Extraordinary Session.

AR - Arkansas Code Annotated > Title 4 Business and Commercial Law > Subtitle 7. Consumer Protection > Chapter 111 Consumer Protection Against Computer Spyware Act

4-111-103. Unlawful acts — Exceptions.

(a) A person that is not an authorized user with actual knowledge, with conscious avoidance of actual knowledge or willfully, shall not cause computer software to be copied onto any computer in this state nor use the software to:

(1) Modify, through intentionally deceptive means, any of the following settings related to the computer's access to, or use of, the internet:

(A) The page which appears when an authorized user launches an internet browser or similar software program used to access and navigate the internet;

(B) The default provider or web proxy the authorized user uses to access or search the internet;

(C) The authorized user's list of bookmarks used to access web pages; or

(D) Settings in computer software or in a text or data file on the computer that are used to resolve a universal resource locator or other location identifier used to access a public or private network;

(2) Collect, through intentionally deceptive means, personally identifiable information about the authorized user that:

(A) Is collected through the use of a keystroke-logging function that records all keystrokes made by an authorized user who uses the computer and transmits the information from the computer to another person;

(B) Includes all or substantially all of the internet addresses visited by an authorized user, other than internet addresses of the provider of the software, if the computer software was installed in an intentionally deceptive manner to conceal from all authorized users of the computer the fact that the software is being installed;

(C) Is extracted from a computer hard drive for a purpose wholly unrelated to any of the purposes of the software or service as described to the authorized user; or

(D) Is collected by extracting screen shots of an authorized user's use of the computer for a purpose wholly unrelated to any of the purposes of the software or service as described to the authorized user;

(3) Prevent without authorization from the authorized user through intentionally deceptive means an authorized user's reasonable efforts to block the installation of or disable software by

causing software that the authorized user has properly removed or disabled to automatically reinstall or reactivate on the computer without the authorization of an authorized user;

(4) Intentionally misrepresent that software will be uninstalled or disabled by an authorized user's action with knowledge that the software will not be uninstalled or disabled; or

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

(b) A person who is not an authorized user who with actual knowledge, with conscious avoidance of actual knowledge, or willfully shall not:

(1) Cause computer software to be copied onto any computer in this state and use the software to take control of a computer by:

(A) Transmitting or relaying without the authorization of an authorized user commercial electronic mail or a computer virus from the consumer's computer;

(B) Accessing or using the authorized user's modem or internet service for the purpose of causing:

(i) Damage to the authorized user's computer; or

(ii) An authorized user to incur financial charges for a service that is not authorized by the authorized user;

(C) 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; or

(D) Opening multiple, sequential, stand-alone advertisements in the authorized user's internet browser without the authorization of an authorized user and with knowledge that a reasonable computer user can not close the advertisements without turning off the computer or closing the authorized user's internet browser;

(2) Without authorization obtain the ability to use one (1) or more computers of other end users on a network to send commercial electronic mail, to damage other computers, or to locate other computers vulnerable to an attack without:

(A) Notice to or knowledge of the owners of the computers or computer networks; or

(B) A prior or existing personal, business, or contractual relationship with the owner or owners of the computer or computer networks;

(3) Modify any of the following settings related to the computer's access to, or use of, the internet:

(A) 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; or

(B) The security settings of the computer for the purpose of causing damage to one (1) or more computers;

(4) Prevent without the authorization of an authorized user an authorized user's reasonable efforts to block the installation of or disable software by 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; or

(5) Intentionally interfere with an authorized user's attempt to uninstall the software by:

(A) Leaving behind without authorization on the authorized user's computer for the purpose of evading an authorized user's attempt to remove the software from the computer hidden elements of the software that are designed to and will reinstall the software or portions of the software;

(B) Intentionally causing damage to or removing any vital component of the operating system;

(C) Falsely representing that software has been disabled;

(D) Changing the name, location, or other designation information of the software for the purpose of preventing an authorized user from locating the software to remove it;

(E) Using randomized or intentionally deceptive file names, directory folders, formats, or registry entries for the purpose of avoiding detection and removal of the software by an authorized user;

(F) Causing the installation of software in a particular computer directory or computer memory for the purpose of evading an authorized user's attempt to remove the software from the computer;

(G) Requiring completion of a survey to uninstall software unless reasonably related to the uninstallation; or

(H) Requiring without the authority of the owner of the computer that an authorized user obtain a special code or download a special program from a third party to uninstall the software.

(c) A person that is not an authorized user, with regard to any computer in this state, shall not:

(1) Induce an authorized user to install a software component onto the computer by intentionally misrepresenting that installing software is necessary for security or privacy reasons or in order to open, view, or play a particular type of content or software; or

(2) Deceptively cause the copying and execution on the computer of a computer software component with the intent of causing an authorized user to use the component in a way that violates any other provision of this section.

(d) No person shall engage in phishing.

(e) A person who is not an authorized user who with actual knowledge, with conscious avoidance of actual knowledge, or willfully shall not cause computer software to be copied onto any computer in this state to carry out any of the violations described in subsections (a)-(d) of this section for a purpose wholly unrelated to any of the purposes of the software or service as described to the authorized user if the software is installed in an intentionally deceptive manner that:

(1) Exploits a security vulnerability in the computer; or

(2) Bundles the software with other software without providing prior notice to the authorized user of the name of the software and that the software will be installed on the computer.

(f) Any provision of a consumer contract that permits an intentionally deceptive practice prohibited under this section is not enforceable.

(g) This section shall not apply to any monitoring of, or interaction with, a subscriber's internet or other network connection or service or a protected computer in accordance with the relationship or agreement between the owner of the computer or computer system used by the authorized user and a:

(1) Telecommunications or internet service provider;

(2) Cable internet provider;

(3) Computer hardware or software provider; or

(4) Provider of information service or interactive computer service for:

(A) Network or computer security purposes;

(B) Diagnostics;

(C) Technical support;

(D) Repair;

(E) Authorized updates of software or system firmware;

(F) Authorized remote system management;

(G) Network management or maintenance; or

(H) Detection or prevention of the unauthorized use or fraudulent or other illegal activities in connection with a network, service, or computer software, including scanning for and removing software proscribed under this subchapter.

(h) Notwithstanding any other provision of this chapter, the provisions of this chapter shall not apply to the installation of:

(1) Software that falls within the scope of a grant of authorization by an authorized user;

(2) An upgrade to a software program that has already been installed on the computer with the authorization of an authorized user; or

(3) Software before the first retail sale and delivery of the computer.

History

Acts 2005, No. 2255, § 1.