

RCW 19.270.020 Unlawful activities—Unauthorized transmission of software. It is unlawful for a person, without the authorization of the owner or operator, to transmit, or procure the transmission of, software to the owner or operator's computer with actual knowledge or conscious avoidance of actual knowledge that the software does any of the following:

(1) Modifies, through deceptive means, settings that control any of the following:

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

(b) The default provider or web proxy the owner or operator uses to access or search the internet;

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

(d) The toolbars or buttons of the owner or operator's internet browser or similar computer software used to access and navigate the internet;

(2) Collects, through intentionally deceptive means, personally identifiable information through the use of a keystroke-logging function or through extracting the information from the owner or operator's hard drive;

(3) Prevents, through intentionally deceptive means, an owner or operator's reasonable efforts to block the installation or execution of, or to disable, computer software;

(4) Misrepresents that computer software will be uninstalled or disabled by an owner or operator's action;

(5) Through intentionally deceptive means, removes, disables, or renders inoperative security, antispyware, or antivirus computer software installed on the computer, or through intentionally deceptive means disables the ability of such computer software to update automatically;

(6) Accesses or uses the modem or internet service for such computer to cause damage to the computer or cause an owner or operator to incur financial charges for a service that is not authorized by the owner or operator;

(7) Opens multiple, sequential, stand-alone advertisements in the owner or operator's computer without the authorization of the owner or operator and that a reasonable computer user cannot close without turning off the computer or closing the internet browser;

(8) Uses the owner or operator's computer as part of an activity performed by a group of computers for the purpose of causing damage to another computer or person including, but not limited to, launching a denial of service attack;

(9) Transmits or relays commercial electronic mail or a computer virus from the owner or operator's computer, where the transmission or relaying is initiated by a person other than the owner or operator;

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

(a) Settings that protect information about the owner or operator in order to make unauthorized use of the owner or operator's personally identifiable information; or

(b) Security settings in order to cause damage to a computer; or

(11) Prevents an owner or operator's reasonable efforts to block the installation of, or to disable, computer software by doing any of the following:

(a) Presenting the owner or operator with an option to decline installation of computer software and with knowledge or conscious avoidance of knowledge that when the option is selected the installation nevertheless proceeds; or

(b) Falsely representing that computer software has been disabled. [2008 c 66 s 2; 2005 c 500 s 2.]