

By the Committee on Commerce and Senator Ring

577-02181A-09

2009164c1

1 A bill to be entitled
2 An act relating to offenses against computer users;
3 amending s. 815.03, F.S.; defining terms for purposes
4 of the Florida Computer Crimes Act; creating s.
5 815.051, F.S.; prohibiting a person who is not an
6 owner or operator of a computer from causing computer
7 software to be copied on a computer knowingly, with
8 conscious avoidance of actual knowledge, or willfully
9 and without authorization taking specified actions
10 with respect to a computer; creating s. 815.053, F.S.;
11 prohibiting a person who is not an owner or operator
12 of a computer from inducing an owner or operator to
13 install a computer software component onto the owner's
14 or operator's computer by deceptively misrepresenting
15 that installing computer software is necessary for
16 security or privacy reasons or by using deceptive
17 means to cause the execution of a computer software
18 component with the intent of causing the computer to
19 use the component in a harmful manner; creating s.
20 815.055, F.S.; providing exceptions; amending s.
21 815.06, F.S.; providing that a violation of the act is
22 a felony of the third degree; providing criminal
23 penalties; providing enhanced criminal penalties under
24 certain circumstances; authorizing the Department of
25 Legal Affairs or a state attorney to file a civil
26 action for injunctive relief against any person or
27 group to restrain prohibited activities; authorizing a
28 court to award court costs and attorney's fees to the
29 prevailing party; permitting a court to impose a civil

577-02181A-09

2009164c1

30 penalty not to exceed a stated amount for each offense
31 against computer users; providing for civil actions by
32 private litigants; providing an effective date.

33
34 Be It Enacted by the Legislature of the State of Florida:

35
36 Section 1. Section 815.03, Florida Statutes, is amended to
37 read:

38 815.03 Definitions.—As used in this chapter, unless the
39 context clearly indicates otherwise:

40 (1) "Access" means to approach, instruct, communicate with,
41 store data in, retrieve data from, or otherwise make use of any
42 resources of a computer, computer system, or computer network.

43 (2) "Cause to be copied" means to distribute or transfer
44 computer software or any component thereof. The term does not
45 include:

46 (a) Transmission, routing, provision of intermediate
47 temporary storage, or caching of software;

48 (b) A storage or hosting medium, such as a compact disk,
49 website, or computer server through which the software was
50 distributed by a third party; or

51 (c) An information-location tool, such as a directory,
52 index, reference, pointer, or hypertext link, through which the
53 user of the computer locates software.

54 (3)~~(2)~~ "Computer" means an internally programmed, automatic
55 device that performs data processing.

56 (4)~~(3)~~ "Computer contaminant" means any set of computer
57 instructions designed to modify, damage, destroy, record, or
58 transmit information within a computer, computer system, or

577-02181A-09

2009164c1

59 computer network without the intent or permission of the owner
60 of the information. The term includes, but is not limited to, a
61 group of computer instructions commonly called viruses or worms
62 which are self-replicating or self-propagating and which are
63 designed to contaminate other computer programs or computer
64 data; consume computer resources; modify, destroy, record, or
65 transmit data; or in some other fashion usurp the normal
66 operation of the computer, computer system, or computer network.

67 (5)~~(4)~~ "Computer network" means any system that provides
68 communications between one or more computer systems and its
69 input or output devices, including, but not limited to, display
70 terminals and printers that are connected by telecommunication
71 facilities.

72 (6)~~(5)~~ "Computer program or computer software" means a set
73 of instructions or statements and related data which, when
74 executed in actual or modified form, cause a computer, computer
75 system, or computer network to perform specified functions.

76 "Computer software" means a sequence of instructions written in
77 any programming language that is executed on a computer.

78 "Computer software" does not include a data component of a web
79 page that is not executable independently of the web page.

80 (7)~~(6)~~ "Computer services" include, but are not limited to,
81 computer time; data processing or storage functions; or other
82 uses of a computer, computer system, or computer network.

83 (8)~~(7)~~ "Computer system" means a device or collection of
84 devices, including support devices, one or more of which contain
85 computer programs, electronic instructions, or input data and
86 output data, and which perform functions, including, but not
87 limited to, logic, arithmetic, data storage, retrieval,

577-02181A-09

2009164c1

88 communication, or control. The term does not include calculators
89 that are not programmable and that are not capable of being used
90 in conjunction with external files.

91 (9) "Computer virus" means a computer program or other set
92 of instructions designed to degrade the performance of or
93 disable a computer or computer network and designed to have the
94 ability to replicate itself on other computers or computer
95 networks without the authorization of the owners of those
96 computers or computer networks.

97 (10) "Damage" means any significant impairment to the
98 integrity or availability of data, software, a system, or
99 information.

100 (11)-~~(8)~~ "Data" means a representation of information,
101 knowledge, facts, concepts, computer software, computer
102 programs, or instructions. Data may be in any form, in storage
103 media or stored in the memory of the computer, or in transit or
104 presented on a display device.

105 (12) "Deceptive" means any of the following:

106 (a) A materially false or fraudulent statement.

107 (b) A statement or description that intentionally omits or
108 misrepresents material information in order to deceive an owner
109 or operator of a computer.

110 (c) A material failure to provide a notice to an owner or
111 operator regarding the installation or execution of computer
112 software for the purpose of deceiving the owner or operator.

113 (13) "Execute," when used with respect to computer
114 software, means the performance of the functions or the carrying
115 out of the instructions of the computer software.

116 (14)-~~(9)~~ "Financial instrument" means any check, draft,

577-02181A-09

2009164c1

117 money order, certificate of deposit, letter of credit, bill of
118 exchange, credit card, or marketable security.

119 (15)~~(10)~~ "Intellectual property" means data, including
120 programs.

121 (16) "Internet" means the global information system that is
122 logically linked together by a globally unique address space
123 based on the Internet protocol (IP), or its subsequent
124 extensions, that is able to support communications using the
125 transmission control protocol/Internet protocol (TCP/IP) suite,
126 or its subsequent extensions, or other IP-compatible protocols,
127 and that provides, uses, or makes accessible, publicly or
128 privately, high-level services layered on the communications and
129 related infrastructure described in this chapter.

130 (17) "Owner or operator" means the owner or lessee of a
131 computer, or a person using such computer with the owner or
132 lessee's authorization, but does not include a person who owned
133 a computer before the first retail sale of the computer.

134 (18) "Message" means a graphical, text, voice, or audible
135 communication presented to an authorized user of a computer.

136 (19) "Person" means any individual, partnership,
137 corporation, limited liability company, or other organization,
138 or any combination thereof.

139 (20) "Personally identifiable information" means any of the
140 following information if it allows the entity holding the
141 information to identify the owner or operator of a computer:

142 (a) The first name or first initial in combination with the
143 last name.

144 (b) A home or other physical address including street name.

145 (c) Personal identification code in conjunction with a

577-02181A-09

2009164c1

146 password required to access an identified account, other than a
147 password, personal identification number, or other
148 identification number transmitted by an authorized user to the
149 issuer of the account or its agent.

150 (d) Social security number, tax identification number,
151 driver's license number, passport number, or any other
152 government-issued identification number.

153 (e) Account balance, bank account number, or credit card
154 numbers, overdraft history, or payment history that personally
155 identifies an owner or operator of a computer.

156 (21)~~(11)~~ "Property" means anything of value as defined in
157 s. 812.011 and includes, but is not limited to, financial
158 instruments, information, including electronically produced data
159 and computer software and programs in either machine-readable or
160 human-readable form, and any other tangible or intangible item
161 of value.

162 Section 2. Section 815.051, Florida Statutes, is created to
163 read:

164 815.051 Prohibitions; use of software.—A person who is not
165 an owner or operator of a computer may not cause computer
166 software to be copied on a computer knowingly, with conscious
167 avoidance of actual knowledge, or willfully, and without
168 authorization, or to use such software to do any of the
169 following:

170 (1) Modify, through deceptive means, settings of a computer
171 which control any of the following:

172 (a) The webpage that appears when an owner or operator
173 launches an Internet browser or similar computer software used
174 to access and navigate the Internet.

577-02181A-09

2009164c1

175 (b) The default provider or web proxy that an owner or
176 operator uses to access or search the Internet.

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

179 (2) Collect, through deceptive means, personally
180 identifiable information through any of the following means:

181 (a) The use of a keystroke-logging function that records
182 all or substantially all keystrokes made by an owner or operator
183 of a computer and transfers that information from the computer
184 to another person.

185 (b) In a manner that correlates personally identifiable
186 information with data regarding all or substantially all of the
187 websites visited by an owner or operator, other than websites
188 operated by the person providing the software, if the computer
189 software was installed in a manner designed to conceal from all
190 authorized users of the computer the fact that the software is
191 being installed.

192 (c) By extracting from the hard drive of an owner's or an
193 operator's computer, an owner's or an operator's social security
194 number, tax identification number, driver's license number,
195 passport number, any other government-issued identification
196 number, account balances, bank account numbers or credit card
197 numbers, or overdraft history for a purpose unrelated to any of
198 the purposes of the software or service described to an
199 authorized user.

200 (3) Prevent, through deceptive means, an owner's or an
201 operator's reasonable efforts to block the installation of or
202 execution of, or to disable, computer software by causing
203 computer software that the owner or operator has properly

577-02181A-09

2009164c1

204 removed or disabled to automatically reinstall or reactivate on
205 the computer without the authorization of an authorized user.

206 (4) Deceptively misrepresent that computer software will be
207 uninstalled or disabled by an owner's or an operator's action.

208 (5) Through deceptive means, remove, disable, or render
209 inoperative security, antispyware, or antivirus computer
210 software installed on an owner's or an operator's computer.

211 (6) Enable the use of an owner's or an operator's computer
212 to do any of the following:

213 (a) Access or use a modem or Internet service for the
214 purpose of causing damage to an owner's or an operator's
215 computer or causing an owner or operator, or a third party
216 affected by such conduct, to incur financial charges for a
217 service that the owner or operator did not authorize.

218 (b) Open multiple, sequential, or stand-alone messages in
219 an owner's or an operator's computer without the authorization
220 of an owner or operator and with knowledge that a reasonable
221 computer user could not close the messages without turning off
222 the computer or closing the software application in which the
223 messages appear; however, this paragraph does not apply to
224 communications originated by the computer's operating system,
225 originated by a software application that the user chooses to
226 activate, originated by a service provider that the user chooses
227 to use, or presented for any of the purposes described in s.
228 815.06(7).

229 (c) Transmit or relay commercial electronic mail or a
230 computer virus from the computer, if the transmission or
231 relaying is initiated by a person other than the authorized user
232 and without the authorization of an authorized user.

577-02181A-09

2009164c1

233 (7) Use deceptive means to modify any of the following
234 settings related the computer's access to, or use of, the
235 Internet:

236 (a) Settings that protect information about an owner or
237 operator for the purpose of obtaining personally identifiable
238 information of the owner or operator.

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

241 (c) Settings that protect the computer from the uses
242 identified in subsection (6).

243 (8) Use deceptive means to prevent, without the
244 authorization of an owner or operator, an owner's or an
245 operator's reasonable efforts to block the installation of, or
246 to disable, computer software by doing any of the following:

247 (a) Presenting the owner or operator with an option to
248 decline installation of computer software with knowledge that,
249 when the option is selected by the authorized user, the
250 installation nevertheless proceeds.

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

253 (c) Requiring in a deceptive manner the user to access the
254 Internet to remove the software with knowledge or reckless
255 disregard of the fact that the software frequently operates in a
256 manner that prevents the user from accessing the Internet.

257 (d) Changing the name, location, or other designation
258 information of the software for the purpose of preventing an
259 authorized user from locating the software in order to remove
260 it.

261 (e) Using randomized or deceptive filenames, directory

577-02181A-09

2009164c1

262 folders, formats, or registry entries for the purpose of
263 avoiding detection and removal of the software by an authorized
264 user.

265 (f) Causing the installation of software in a particular
266 computer directory or computer memory for the purpose of evading
267 authorized users' attempts to remove the software from the
268 computer.

269 (g) Requiring, without the authority of the owner of the
270 computer, that an authorized user obtain a special code or
271 download software from a third party in order to uninstall the
272 software.

273 Section 3. Section 815.053, Florida Statutes, is created to
274 read:

275 815.053 Other prohibitions.—A person who is not an owner or
276 operator of a computer may not do any of the following with
277 regard to the computer:

278 (1) Induce an owner or operator to install a computer
279 software component onto the owner's or operator's computer by
280 deceptively misrepresenting that installing computer software is
281 necessary for security or privacy reasons or in order to open,
282 view, or play a particular type of content.

283 (2) Using deceptive means to cause the execution of a
284 computer software component with the intent of causing the
285 computer to use such component in a manner that violates any
286 other provision of this chapter.

287 Section 4. Section 815.055, Florida Statutes, is created to
288 read:

289 815.055 Exceptions.—

290 (1) Sections 815.051 and 815.053 do not apply to the

577-02181A-09

2009164c1

291 monitoring of, or interaction with, an owner's or an operator's
292 Internet or other network connection, service, or computer by a
293 telecommunications carrier, cable operator, computer hardware or
294 software provider, or provider of information service or
295 interactive computer service for purposes of network or computer
296 security, diagnostics, technical support, maintenance, repair,
297 network management, authorized updates of computer software or
298 system firmware, authorized remote system management, or
299 detection or prevention of the unauthorized use of, or
300 fraudulent or other illegal activities in connection with, a
301 network, service, or computer software, including scanning for
302 and removing computer software proscribed under this chapter.

303 (2) This section does not provide a defense to liability
304 under the common law or any other state or federal law, and may
305 not be construed to be an affirmative grant of authority to
306 engage in any of the activities listed in this section.

307 (3) This section does not impose liability on any
308 communications service providers as defined in s. 202.11(2),
309 commercial mobile service providers, or providers of information
310 services, including, but not limited to, Internet access service
311 providers and hosting service providers, if they provide the
312 transmission, storage, or caching of electronic communications
313 or messages of others or provide other related
314 telecommunications, commercial mobile radio service, or
315 information services used by others in violation of this
316 chapter. This exemption from liability is consistent with and in
317 addition to any liability exemption provided under 47 U.S.C. s.
318 230.

319 (4) This section does not prohibit or criminalize the use

577-02181A-09

2009164c1

320 of software by parents or guardians to monitor Internet or
321 computer usage of their minor children.

322 Section 5. Section 815.06, Florida Statutes, is amended to
323 read:

324 815.06 Offenses against computer users.—

325 (1) Whoever willfully, knowingly, and without
326 authorization:

327 (a) Accesses or causes to be accessed any computer,
328 computer system, or computer network;

329 (b) Disrupts or denies or causes the denial of computer
330 system services to an authorized user of such computer system
331 services, which, in whole or part, is owned by, under contract
332 to, or operated for, on behalf of, or in conjunction with
333 another;

334 (c) Destroys, takes, injures, or damages equipment or
335 supplies used or intended to be used in a computer, computer
336 system, or computer network;

337 (d) Destroys, injures, or damages any computer, computer
338 system, or computer network; ~~or~~

339 (e) Violates s. 815.051 or s. 815.053; or

340 (f)~~(e)~~ Introduces any computer contaminant into any
341 computer, computer system, or computer network,

342
343 commits an offense against computer users.

344 (2) (a) Except as provided in paragraphs (b) and (c),
345 whoever violates subsection (1) commits a felony of the third
346 degree, punishable as provided in s. 775.082, s. 775.083, or s.
347 775.084.

348 (b) Whoever violates subsection (1) and:

577-02181A-09

2009164c1

349 1. Damages a computer, computer equipment, computer
350 supplies, a computer system, or a computer network, and the
351 monetary damage or loss incurred as a result of the violation is
352 \$5,000 or greater;

353 2. Commits the offense for the purpose of devising or
354 executing any scheme or artifice to defraud or obtain property;
355 or

356 3. Interrupts or impairs a governmental operation or public
357 communication, transportation, or supply of water, gas, or other
358 public service,

359
360 commits a felony of the second degree, punishable as provided in
361 s. 775.082, s. 775.083, or s. 775.084.

362 (c) Whoever violates subsection (1) and the violation
363 endangers human life commits a felony of the first degree,
364 punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

365 (3) Whoever willfully, knowingly, and without authorization
366 modifies equipment or supplies used or intended to be used in a
367 computer, computer system, or computer network commits a
368 misdemeanor of the first degree, punishable as provided in s.
369 775.082 or s. 775.083.

370 (4) The Department of Legal Affairs or a state attorney may
371 file a civil action on behalf of the people of this state for
372 injunctive relief against any person or group violating
373 subsection (1) to restrain the prohibited activity. The court
374 may award court costs and reasonable attorney's fees to the
375 prevailing party. The court may also impose a civil penalty that
376 may not exceed \$10,000 for each violation of subsection (1), and
377 the total penalties may not exceed \$1 million per defendant.

577-02181A-09

2009164c1

378 (5)~~(4)~~(a) In addition to any other civil remedy available,
379 the owner or lessee of the computer, computer system, computer
380 network, computer program, computer equipment, computer
381 supplies, or computer data may bring a civil action against any
382 person convicted under this section for compensatory damages.

383 (b) In any action brought under this subsection, the court
384 may award reasonable attorney's fees to the prevailing party.

385 (6)~~(5)~~ Any computer, computer system, computer network,
386 computer software, or computer data owned by a defendant which
387 is used during the commission of any violation of this section
388 or any computer owned by the defendant which is used as a
389 repository for the storage of software or data obtained in
390 violation of this section is subject to forfeiture as provided
391 under ss. 932.701-932.704.

392 (7)~~(6)~~ This section does not apply to any person who
393 accesses his or her employer's computer system, computer
394 network, computer program, or computer data when acting within
395 the scope of his or her lawful employment.

396 (8)~~(7)~~ For purposes of bringing a civil or criminal action
397 under this section, a person who causes, by any means, the
398 access to a computer, computer system, or computer network in
399 one jurisdiction from another jurisdiction is deemed to have
400 personally accessed the computer, computer system, or computer
401 network in both jurisdictions.

402 (9) This section does not prohibit a private litigant from
403 filing a civil action for damages arising under this section.

404 Section 6. This act shall take effect July 1, 2009.