

A.R.S. § 13-2316

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 13 Criminal Code (Chs. 1 — 46) > Chapter 23 Organized Crime, Fraud and Terrorism (§§ 13-2301 — 13-2323)

13-2316. Computer tampering; venue; forfeiture; classification

A. A person who acts without authority or who exceeds authorization of use commits computer tampering by:

1. Accessing, altering, damaging or destroying any computer, computer system or network, or any part of a computer, computer system or network, with the intent to devise or execute any scheme or artifice to defraud or deceive, or to control property or services by means of false or fraudulent pretenses, representations or promises.
2. Knowingly altering, damaging, deleting or destroying computer programs or data.
3. Knowingly introducing a computer contaminant into any computer, computer system or network.
4. Recklessly disrupting or causing the disruption of computer, computer system or network services or denying or causing the denial of computer or network services to any authorized user of a computer, computer system or network.
5. Recklessly using a computer, computer system or network to engage in a scheme or course of conduct that is directed at another person and that seriously alarms, torments, threatens or terrorizes the person. For the purposes of this paragraph, the conduct must both:
 - (a) Cause a reasonable person to suffer substantial emotional distress.
 - (b) Serve no legitimate purpose.
6. Preventing a computer user from exiting a site, computer system or network-connected location in order to compel the user's computer to continue communicating with, connecting to or displaying the content of the service, site or system.
7. Knowingly obtaining any information that is required by law to be kept confidential or any records that are not public records by accessing any computer, computer system or network that is operated by this state, a political subdivision of this state, a health care provider as defined in section 12-2291, a clinical laboratory as defined in section 36-451 or a person or entity that provides services on behalf of a health care provider or a clinical laboratory.
8. Knowingly accessing any computer, computer system or network or any computer software, program or data that is contained in a computer, computer system or network.

B. In addition to section 13-109, a prosecution for a violation of this section may be tried in any of the following counties:

1. The county in which the victimized computer, computer system or network is located.
 2. The county in which the computer, computer system or network that was used in the commission of the offense is located or in which any books, records, documents, property, financial instruments, computer software, data, access devices or instruments of the offense were used.
 3. The county in which any authorized user was denied service or in which an authorized user's service was interrupted.
 4. The county in which critical infrastructure resources were tampered with or affected.
- C.** On conviction of a violation of this section, the court shall order that any computer system or instrument of communication that was owned or used exclusively by the defendant and that was used in the commission of the offense be forfeited and sold, destroyed or otherwise properly disposed.
- D.** A violation of subsection A, paragraph 6 of this section constitutes an unlawful practice under section 44-1522 and is in addition to all other causes of action, remedies and penalties that are available to this state. The attorney general may investigate and take appropriate action pursuant to title 44, chapter 10, article 7.
- E.** Computer tampering pursuant to subsection A, paragraph 1 of this section is a class 3 felony. Computer tampering pursuant to subsection A, paragraph 2, 3 or 4 of this section is a class 4 felony, unless the computer, computer system or network tampered with is a critical infrastructure resource, in which case it is a class 2 felony. Computer tampering pursuant to subsection A, paragraph 5 of this section is a class 5 felony. Computer tampering pursuant to subsection A, paragraph 7 or 8 of this section is a class 6 felony.

History

Laws 1993, 1st Reg. Sess., Ch. 257, § 1; Laws 1995, 1st Reg. Sess., Ch. 142, § 1; Laws 2000, Ch. 189, § 10; Laws 2011, 1st Reg. Sess., Ch. 268, § 4.