

## Code of Ala. § 13A-8-112

Current through the end of the 2023 First Special, Regular, and Second Special Sessions, but not including corrections and changes made to the 2023 session laws by the Code Commissioner.

*Michie's™ Alabama Code > TITLE 13A Criminal Code (Chs. 1 — 14) > CHAPTER 8 Offenses Involving Theft (Arts. 1 — 11) > Article 5A The Alabama Digital Crime Act (§§ 13A-8-110 — 13A-8-119)*

### **§ 13A-8-112. Computer tampering.**

---

(a) A person who acts without authority or who exceeds authorization of use commits the crime of computer tampering by knowingly:

- (1) Accessing and altering, damaging, or destroying any computer, computer system, or computer network.
- (2) Altering, damaging, deleting, or destroying computer programs or data.
- (3) Disclosing, using, controlling, or taking computer programs, data, or supporting documentation residing in, or existing internal or external to, a computer, computer system, or network.
- (4) Directly or indirectly introducing a computer contaminator or a virus into any computer, computer system, or network.
- (5) Disrupting or causing the disruption of a 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.
- (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) 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, or a medical institution.
- (8) Giving a password, identifying code, personal identification number, debit card number, bank account number, or other confidential information about a computer security system to another person without the consent of the person using the computer security system to restrict access to a computer, computer network, computer system, or data.

(b)

- (1) Except as otherwise provided in this subsection, the offense of computer tampering is a Class A misdemeanor, punishable as provided by law. Subsection (a) does not apply to any acts which are committed by a person within the scope of his or her lawful employment. For purposes of this section, a person acts within the scope of his or her employment when he or she performs acts which are reasonably necessary to the performance of his or her work assignment.

## § 13A-8-112. Computer tampering.

- (2) If the actor's intent is to commit an unlawful act or obtain a benefit, or defraud or harm another, the offense is a Class C felony, punishable as provided by law.
- (3) If any violation results in a victim expenditure of greater than two thousand five hundred dollars (\$2,500), or if the actor's intent is to obtain a benefit, commit an unlawful act, or defraud or harm another and there is an interruption or impairment of governmental operations or public communication, transportation, or supply of water, gas, or other public or utility service, the offense is a Class B felony, punishable as provided by law.
- (4) If any violation results in a victim expenditure of greater than one hundred thousand dollars (\$100,000), or if the committed offense causes physical injury to any person who is not involved in the act, the offense is a Class A felony, punishable as provided by law.
- (5) If any violation relates to access to an Alabama Criminal Justice Information Center information system or to data regulated under the authority of the Alabama Criminal Justice Information Center Commission, the offense is a Class B felony, punishable as provided by law. Misuse of each individual record constitutes a separate offense under this subsection.
- (c) A prosecution for a violation of this section may be tried in any of the following:
- (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.

## History

---

Acts 2012, No. 12-432, § 3, Aug. 1, 2012.

Michie's™ Alabama Code  
Copyright © 2024 Matthew Bender & Company, Inc.,  
a member of the LexisNexis Group. All rights reserved.

---

End of Document