The Computer Fraud And Abuse Act A Guide For General Counsels And Cios

Cyber crime : updating the Computer Fraud and Abuse Act to protect cyber space and combat emerging threats : hearing before the Committee on the Judiciary, United States Senate, One Hundred Twelfth Congress, first session, September 7, 2011.

Cyber crime: updating the Computer Fraud and Abuse Act to protect cyber space and combat emerging threats : hearing before the Committee on the Judiciary, United States Senate, One Hundred Twelfth Congress, first session, September 7, 2011.

Intellectual Property and Computer Crimes examines criminal infringement, the expanded scope of computer hacking laws, and the important legal issues that arise when these crimes are prosecuted.

This one-of-a-kind collection consists of actual cases written by fraud examiners out in the field. These cases were hand selected from hundreds of submissions and together form a comprehensive picture of the many types of computer fraud how they are investigated, across industries and throughout the world. Topics included are email fraud, on-line auction fraud, security breaches, counterfeiting, and others.

The bestselling cyberpunk author “has produced by far the most stylish report from the computer outlaw culture since Steven Levy’s Hackers” (Publishers Weekly). Bruce Sterling delves into the world of high-tech crime and punishment in one of the first books to explore the cyberspace breaches that threaten national security. From the crash of AT&T’s long-distance switching system to corporate cyberattacks, he investigates government and law enforcement efforts to break the back of America’s electronic underground in the 1990s. In this modern classic, “Sterling makes the hackers—who live in the ether between terminals under noms de net such as VaxCat—as vivid as Wyatt Earp and Doc Holliday. His book goes a long way towards explaining the emerging digital world and its ethos” (Publishers Weekly). This edition features a new preface by the author that analyzes the sobering increase in computer crime over the twenty-five years since The Hacker Crackdown was first published. “Offbeat and brilliant.” —Booklist “Thoroughly researched, this account of the government’s crackdown on the nebulous but growing computer-underground provides a thoughtful report on the laws and rights being defined on the virtual frontier of cyberspace. . . . An enjoyable, informative, and (as the first mainstream treatment of the subject) potentially important book . . . Sterling is a fine and knowledgeable guide to this strange new world.” —Kirkus Reviews “A well-balanced look at this new group of civil libertarians. Written with humor and intelligence, this book is highly recommended.” —Library Journal

The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030, outlaws conduct that victimizes computer systems. It is a cyber security law. It protects federal computers, bank computers, and computers connected to the Internet. It shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud. It is not a comprehensive provision, but instead it fills cracks and gaps in the protection afforded by other federal criminal laws. This is a brief sketch of CFAA and some of its federal statutory companions, including the amendments found in the Identity Theft Enforcement and Restitution Act, P.L. 110-326, 122 Stat. 3560 (2008). This report is available in abbreviated form—without the footnotes, citations, quotations, or appendixes found in this report—under the title CRS Report RS20830, Cybercrime: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws, by Charles

Doyle.

Cybercrime and Digital Deviance is a work that combines insights from sociology, criminology, and computer science to explore cybercrimes such as hacking and romance scams, along with forms of cyberdeviance such as pornography addiction, trolling, and flaming. Other issues are explored including cybercrime investigations, organized cybercrime, the use of algorithms in policing, cybervictimization, and the theories used to explain cybercrime. Graham and Smith make a conceptual distinction between a terrestrial, physical environment and a single digital environment produced through networked computers. Conceptualizing the online space as a distinct environment for social interaction links this text with assumptions made in the fields of urban sociology or rural criminology. Students in sociology and criminology will have a familiar entry point for understanding what may appear to be a technologically complex course of study. The authors organize all forms of cybercrime and cyberdeviance by applying a typology developed by David Wall: cybertrespass, cyberdeception, cyberviolence, and cyberpornography. This typology is simple enough for students just beginning their inquiry into cybercrime. Because it is based on legal categories of trespassing, fraud, violent crimes against persons, and moral transgressions it provides a solid foundation for deeper study. Taken together, Graham and Smith’s application of a digital environment and Wall’s cybercrime typology makes this an ideal upper level text for students in sociology and criminal justice. It is also an ideal introductory text for students within the emerging disciplines of cybercrime and cybersecurity.

Looks at the federal computer fraud and abuse statute.

Computer Fraud & Abuse Laws An Overview Of Federal Criminal Laws

The federal computer fraud and abuse statute, 18 U.S.C. 1030, outlaws conduct that victimizes computer systems. It is a cyber security law which protects federal computers, bank computers, and computers connected to the Internet. It shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud. It is not a comprehensive provision, but instead it fills cracks and gaps in the protection afforded by other federal criminal laws. This report provides a brief sketch of Section 1030 and some of its federal statutory companions, including the amendments found in the Identity Theft Enforcement and Restitution Act, P.L. 110-326. Extensive appendices. This is a print on demand publication.

CybercrimeAn Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal LawsDIANE Publishing

Companies and other organizations have always had to face the problem of fraud. However, this threat to commercial success has taken on a new dimension with the development of computer-based systems. Today, the criminal is often adept at coping with the obstacles posed to his activities by electronic facilities in the office and other business environments.

This fully-updated, integrated self-study system offers complete coverage of the revised 2015 Systems Security Certified Practitioner (SSCP) exam domains Thoroughly revised for the April 2015 exam update, SSCP Systems Security Certified Practitioner All-in-One Exam Guide, Second Edition enables you to take the exam with complete confidence. To aid in self-study, each chapter includes Exam Tips that highlight key exam information, chapter summaries that reinforce salient points, and end-of-chapter questions that are an accurate reflection of the content and question format of the real exam. Beyond exam prep, the practical examples and real-world insights offered in this guide make it an ideal on-the-job reference for IT security professionals. You will learn the security concepts, tools, and procedures needed to employ and enforce solid security policies and effectively react to security incidents. Features 100% coverage of the revised SSCP Common Body of Knowledge (CBK), effective April 2015 CD-ROM contains two full-length, customizable practice exams in the Total Tester exam engine and a searchable PDF copy of the book Written by a bestselling IT security certification and training expert

This book is concerned with the nature of computer misuse and the legal and extra-legal responses to it. It explores what is meant by the term 'computer misuse' and charts its emergence as a problem as well as its expansion in parallel with the continued progression in computing power, networking, reach and accessibility. In doing so, it surveys the attempts of the domestic criminal law to deal with some early manifestations of computer misuse and the consequent legislative passage of the Computer Misuse Act 1990. This book will be of interest to students of IT law as well as to sociologists and criminologists, and those who have a professional concern with preventing computer misuse and fraud.