Cyber Crime

Yeah, reviewing a book **Cyber Crime** could grow your close connections listings. This is just one of the solutions for you to be successful. As understood, finishing does not recommend that you have fabulous points.

Comprehending as without difficulty as harmony even more than new will meet the expense of each success. neighboring to, the notice as competently as acuteness of this Cyber Crime can be taken as capably as picked to act.

Cybercrime - Ralph D. Clifford 2011
Cybercrime is a legal workbook for anyone involved in the rapidly developing area of cybercrime. It comprehensively covers: determining what conduct is considered a cybercrime, investigating improper cyber conduct, trying a cybercrime case as a prosecuting or defending attorney, and handling the international aspects of cybercrime. As technology grows increasingly complex, so does computer crime. In this third edition, Clifford leads a team of nationally known experts in cybercrime (gathered from the diverse fields of academia, private, and governmental practice) to unfold the legal mysteries of computer crime. The book explores the variety of crimes that involve computer technology and provides essential details on procedural and tactical issues associated with the prosecution and defense of a cybercrime. The authors' insight will be of great interest to criminal prosecution and defense attorneys, law enforcement officers, and students of computer or modern criminal law.
Principles of Cybercrime - Jonathan Clough 2015-09-24
A comprehensive doctrinal analysis of cybercrime laws in four major common law jurisdictions: Australia, Canada, the UK and the US.
Cyber Crime Investigations - Anthony Reyes 2011-04-18
Written by a former NYPD cyber cop, this is the only book available that discusses the hard questions cyber crime investigators are asking. The book begins with the chapter “What is Cyber Crime? This introductory chapter describes the most common challenges faced by cyber investigators today. The following chapters discuss the methodologies behind cyber investigations; and frequently encountered pitfalls. Issues relating to cyber crime definitions, the electronic crime scene, computer forensics, and preparing and presenting a cyber crime investigation in court will be examined. Not only will these topics be generally be discussed and explained for the novice, but the hard questions —the questions that have the power to divide this community— will also be examined in a comprehensive and thoughtful manner. This book will serve as a foundational text for the cyber crime community to begin to move past current difficulties into its next evolution. This book has been written by a retired NYPD cyber cop, who has worked many high-profile computer crime cases Discusses the complex relationship between the public and private sector with regards to cyber crime Provides essential information for IT security professionals and first responders on maintaining chain of evidence
Cyber-Crime - Rod Broadhurst 2005-05-01
This collection is innovative and original. It introduces new knowledge and is very timely because of the current high profile of the international public discourse over security, the internet and its impact upon the growth of the information economy. The book will be very useful to a wide range of readers because it will both inform and provide the basis for instruction. This book significantly advances the scholarly literature available on the global problem of cyber-crime. It also makes a unique contribution to the literature in this area. Much of what has been written focuses on cyber-crime in the United States and in Europe. This much-needed volume focuses on how cyber-crime is being dealt with in Asian countries. It explains how law enforcement is responding to the complex issues cyber-crime raises and analyzes the difficult policy issues this new type of transnational crime generates. This book is an invaluable addition to the library of anyone who is concerned about online crime, computer security or the emerging culture of the Internet.
Cybercrime and its victims - Elena Martellozzo 2017-06-26
The last twenty years have seen an explosion in the development of information technology, to the point that people spend a major portion of waking life in online spaces. While there are enormous benefits associated with this technology, there are also risks that can affect the most vulnerable in our society but also the most confident. Cybercrime and its victims explores the social construction of violence and victimisation in online spaces and brings together scholars from many areas of inquiry, including criminology, sociology, and cultural, media, and gender studies. The book is organised thematically into five parts. Part one addresses some broad conceptual and theoretical issues. Part two is concerned with issues relating to sexual violence, abuse, and exploitation, as well as to sexual expression online. Part three addresses issues related to race and culture. Part four addresses concerns around cyberbullying and online suicide, grouped together as ‘social violence’. The final part argues that victims of cybercrime are, in general, neglected and not receiving the recognition and support they need and deserve. It concludes that in the volatile and complex world of cyberspace continued awareness-raising is essential for bringing attention to the plight of victims. It also argues that there needs to be more support of all kinds for victims, as well as an increase in the exposure and punishment of perpetrators. Drawing on a range of pressing contemporary issues such as online grooming, sexting, cyber-hate, cyber-bulling and online radicalization, this book examines how cyberspace makes us more vulnerable to crime and violence, how it gives rise to new forms of surveillance and social control and how cybercrime can be prevented.
Cybercrime and Society - Majid Yar 2006-06
Providing a clear and systematic introduction to current debates surrounding cybercrime, this text looks at a range of issues including computer hacking, cyber-terrorism, media 'piracy' and online stalking.
Cyber Crime - Catherine D. Marcum 2022-04-19
Cybercrime, Investigating the Shadows of the Internet Cybercrime provides the reader with a thorough examination of the prominence of cybercrime in our society, as well as the criminal justice system experience with cybercrimes. Research from scholars in the academic field, as well as government studies, statutes, and other material are gathered and summarized. Key concepts, statistics, and legislative histories are discussed in every chapter. The book is meant to educate and enlighten a wide audience, from those who are completely unfamiliar with the topic as an entirety, to individuals who need more specific information on a particular type of cybercrime. This text should be a useful guide to students, academics, and practitioners alike. New to the Third Edition: In-depth discussions of the dark web New coverage of child sexual abuse material (CSAM) Discussions of fraud related to government aid during the coronavirus epidemic Extensive updates to the issues of underage sexting and nonconsensual pornography New case studies to encompass recent developments in the areas of: child pornography and solicitation the Internet and prostitution revenge pornography efforts to combat piracy cyberbullying ransomware, hacking, and governmental relations terrorists’ use of social media Updated statistics that reflect the latest data Professors and students will benefit from: Case studies in each chapter that connect new concepts to current events and illustrate the use of criminal theory in crime solving Questions for discussion that encourage evaluative and analytical thinking Discussion and analysis of the demographics and characteristics of the offenders and their victims An informative review of the efforts of legislation, public policy, and law enforcement to prevent and prosecute cybercrime Coverage of the most widespread and damaging types of cybercrime intellectual property theft online sexual victimization identity theft cyberfraud and financial crimes harassment
Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Joshua B. Hill 2016-02-22
Explaining cybercrime in a highly networked world, this book provides a comprehensive yet accessible summary of the history, modern developments, and efforts to combat cybercrime in various forms at all levels of government—international, national, state, and local. • Provides accessible, comprehensive coverage of a complex topic that encompasses identity theft to copyright infringement written for non-technical readers • Pays due attention to important elements of cybercrime that have been largely ignored in the field, especially politics • Supplies examinations of both the domestic and international efforts to combat cybercrime • Serves an ideal text for first-year undergraduate students in criminal justice programs
Cybercrime - Robert Moore 2014-09-25

This innovative text provides an excellent introduction to technology-assisted crime and the basics of investigating such crime, from the criminal justice perspective. It presents clear, concise explanations for students and professionals, who need not be technically proficient to find the material easy-to-understand and practical. The book begins by identifying and defining the most prevalent and emerging high-technology crimes — and exploring their history, their original methods of commission, and their current methods of commission. Then it delineates the requisite procedural issues associated with investigating technology-assisted crime. In addition, the text provides a basic introduction to computer forensics, explores legal issues in the admission of digital evidence, and then examines the future of high-technology crime, including legal responses.

Cyber Crime: Concepts, Methodologies, Tools and Applications - Management Association, Information Resources 2011-11-30

Threatening the safety of individuals, computers, and entire networks, cyber crime attacks vary in severity and type. Studying this continually evolving discipline involves not only understanding different types of attacks, which range from identity theft to cyberwarfare, but also identifying methods for their prevention. Cyber Crime: Concepts, Methodologies, Tools and Applications is a three-volume reference that explores all aspects of computer-based crime and threats, offering solutions and best practices from experts in software development, information security, and law. As cyber crime continues to change and new types of threats emerge, research focuses on developing a critical understanding of different types of attacks and how they can best be managed and eliminated.

Cyber Crime and Digital Disorder - P. Madhava Soma Sundaram and Syed Umarhathab 2011

The Elite Cyber Criminals' Stories - A. J. WRIGHT 2020-09-27

This book is the product of my 7-year human cybercriminal project. It is a must read if you want to update your knowledge about the latest cyber crime techniques. You can use this book to do extensive research and learn various ways of protecting your organization or business from cyber attacks, especially if you're working or learning from home. I spent the last 7 years traveling to 20 different cybercrime hotspots around the world. A few of them are Russia, Ukraine, Romania, Nigeria, Brazil, USA and China. I traveled to these places to try and understand how the organization of cybercrime works, and to get a bit more of an informed opinion about it. That's quite a standard way sociologists do things. What I did over the 7-year period is I interviewed 240 different people, including law enforcement backgrounds, the private sectors who're involved in tracking this type of activity, and then also cybercriminals. The purposes of this is to put all this information together in this book, to make you know the truth, and understand more about cyber crime.

Introduction to Cyber Crime - Mark Sherman 2000

Cybercrime in Progress - Thomas J Holt 2015-12-14

The emergence of the World Wide Web, smartphones, and computers has transformed the world and enabled individuals to engage in crimes in a multitude of new ways. Criminological scholarship on these issues has increased dramatically over the last decade, as have studies on ways to prevent and police these offenses. This book is one of the first texts to provide a comprehensive review of research regarding cybercrime, policing and enforcing these offenses, and the prevention of various offenses as global change and technology adoption increases the risk of victimization around the world. Drawing on a wide range of literature, Holt and Bossler offer an extensive synthesis of numerous contemporary topics such as theories used to account for cybercrime, policing in domestic and transnational contexts, cybercrime victimization and issues in cybercrime prevention. The findings provide a roadmap for future research in cybercrime, policing, and technology, and discuss key controversies in the existing research literature in a way that is otherwise absent from textbooks and general cybercrime readers. This book is an invaluable resource for academics, practitioners, and students interested in understanding the state of the art in social science research. It will be of particular interest to scholars and students interested in cybercrime, cyber-deviance, victimization, policing, criminological theory, and technology in general.

Cybercrime and Society - Majid Yar 2019-02-25

The Third Edition of Cybercrime and Society provides readers with expert analysis on the most important cybercrime issues affecting modern society. The book has undergone extensive updates and expands on the topics addressed in the 2013 edition, with updated analysis and contemporary case studies on subjects such as: computer hacking, cyberterrorism, hate speech, internet pornography, child sex abuse, and policing the internet. New author Kevin Steinmetz brings further expertise to the book, including an in-depth insight into computer hacking. The third edition also includes two new chapters: “Researching and Theorizing Cybercrime” explains how criminological theories have been applied to various cybercrime issues, and also highlights the challenges facing the academic study of cybercrime. “Looking toward the Future of Cybercrime” examines the implications for future cybercrimes, including biological implants, cloud-computing, state-sponsored hacking and propaganda, and the effects online regulation would have on civil liberties. The book is supported by online resources for lecturers and students, including: Lecturer slides, Multiple-choice questions, web links, Podcasts, and exclusive SAGE Videos. Suitable reading for undergraduates and postgraduates studying cybercrime and cybersecurity.

The Psychology of Cyber Crime: Concepts and Principles - Kirwan, Gráinne 2011-11-30

As more individuals own and operate Internet-enabled devices and more critical government and industrial systems rely on advanced technologies, the issue of cybercrime has become a crucial concern for both the general public and professionals alike. The Psychology of Cyber Crime: Concepts and Principles aims to be the leading reference examining the psychology of cybercrime. This book considers many aspects of cybercrime, including research on offenders, legal issues, the impact of cybercrime on victims, punishment, and preventative measures. It is designed as a source for researchers and practitioners in the disciplines of criminology, cyberpsychology, and forensic psychology, though it is also likely to be of significant interest to many students of information technology and other related disciplines.

Cyberspace, Cybersecurity, and Cybercrime - Janine Kremling 2017-09-05

Presented from a criminal justice perspective, Cyberspace, Cybersecurity, and Cybercrime introduces students to the interdisciplinary field of cybercrime by exploring the theoretical, practical, and legal framework it operates under, along with strategies to combat it. Authors Janine Kremling and Amanda M. Sharp Parker provide a straightforward overview of cybercrime, cyberthreats, and the vulnerabilities individuals, businesses, and governments face everyday in a digital environment. Highlighting the latest empirical research findings and challenges that cybercrime and cybersecurity pose for those working in the field of criminal justice, this book exposes critical issues related to privacy, terrorism, hacktivism, the dark web, and much more. Focusing on the past, present, and future impact of cybercrime and cybersecurity, it details how criminal justice professionals can be prepared to confront the changing nature of cybercrime. Instructors! Sign in at study.sagepub.com/kremling for PowerPoint slides, test banks, and more!

Cyber Crime - Nash Haynes 2018-11-07

Cyber Crime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants is being run on computers, Cyber Crime has assumed rather sinister implications. Cyber Crime poses great challenges for law enforcement and for society in general. To understand why this is true, it is necessary to understand why, and how, cybercrime differs from traditional, terrestrial crime. Net-crime refers to criminal use of the Internet. Cyber-crimes are essentially a combination of these two elements and can be best defined as "e;Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly using modern telecommunication networks such as the Internet (Chat rooms, e-mails, notice boards and groups) and mobile phones (SMS/MMS)"e;. Since Cyber Crime is a newly specialized field, growing in cyber laws, there is absolutely no comprehensive law on Cyber Crime anywhere in the world. This is precisely the reason why investigating agencies are finding cyberspace to be an extremely difficult terrain to handle. This book explores technical, legal, and social issues related to Cyber Crime. Cyber Crime is a broad term that includes offences where a computer may be the target, crimes where a computer may be a tool used in the commission of an existing offence, and crimes where a computer may play a subsidiary role such as offering evidence for the commission of an offence.

Cyber crime strategy - Great Britain: Home Office 2010-03-30

The Government published the UK Cyber Security Strategy in June 2009 (Cm. 7642, ISBN 9780101767423), and established the Office of Cyber Security to provide strategic leadership across Government. This

document sets out the Home Office's approach to tackling cyber crime, showing how to tackle such crimes directly through the provision of a law enforcement response, and indirectly through cross-Government working and through the development of relationships with industry, charities and other groups, as well as internationally. The publication is divided into five chapters and looks at the following areas, including: the broader cyber security context; cyber crime: the current position; the Government response and how the Home Office will tackle cyber crime.

Cybercrime and Espionage - Will Gragido 2011-01-07

Cybercrime and Espionage provides a comprehensive analysis of the sophisticated patterns and subversive multi-vector threats (SMTs) associated with modern cybercrime, cyber terrorism, cyber warfare and cyber espionage. Whether the goal is to acquire and subsequently sell intellectual property from one organization to a competitor or the international black markets, to compromise financial data and systems, or undermine the security posture of a nation state by another nation state or sub-national entity, SMTs are real and growing at an alarming pace. This book contains a wealth of knowledge related to the realities seen in the execution of advanced attacks, their success from the perspective of exploitation and their presence within all industry. It will educate readers on the realities of advanced, next generation threats, which take form in a variety ways. This book consists of 12 chapters covering a variety of topics such as the maturity of communications systems and the emergence of advanced web technology; how regulatory compliance has worsened the state of information security; the convergence of physical and logical security; asymmetric forms of gathering information; seven commonalities of SMTs; examples of compromise and presence of SMTs; next generation techniques and tools for avoidance and obfuscation; and next generation techniques and tools for detection, identification and analysis. This book will appeal to information and physical security professionals as well as those in the intelligence community and federal and municipal law enforcement, auditors, forensic analysts, and CIO/CSO/CISO. Includes detailed analysis and examples of the threats in addition to related anecdotal information Authors' combined backgrounds of security, military, and intelligence, give you distinct and timely insights Presents never-before-published information: identification and analysis of cybercrime and the psychological profiles that accompany them

Cybercrime and Cloud Forensics: Applications for Investigation Processes - Ruan, Keyun 2012-12-31

While cloud computing continues to transform developments in information technology services, these advancements have contributed to a rise in cyber attacks; producing an urgent need to extend the applications of investigation processes. Cybercrime and Cloud Forensics: Applications for Investigation Processes presents a collection of research and case studies of applications for investigation processes in cloud computing environments. This reference source brings together the perspectives of cloud customers, security architects, and law enforcement agencies in the developing area of cloud forensics.

Digital Crime Investigation - Benild Joseph 2017-11-11

"Digital Crime Investigation" written by Benild Joseph gives an insight to investigators helping them with the background and tools that they need to investigate crime occurring in the digital world. This extremely useful guide provides step-by-step instructions for investigating Internet crimes, including locating, interpreting, understanding, collecting, and documenting online electronic evidence to assist investigations.Law enforcement departments and security officers all over the world having the responsibility for enforcing, investigating and prosecuting cybercrime are overpowered, not only with the increasing number of crimes being committed but also by a lack of adequate training material. This book provides that fundamental knowledge, including how to properly collect and document online evidence, trace IP addresses, and work undercover.

Encyclopedia of Cybercrime - Samuel C. McQuade III 2008-11-30

There are today no more compelling sets of crime and security threats facing nations, communities, organizations, groups, families and individuals than those encompassed by cybercrime. For over fifty years crime enabled by computing and telecommunications technologies have increasingly threatened societies as they have become reliant on information systems for sustaining modernized living. Cybercrime is not a new phenomenon, rather an evolving one with respect to adoption of information technology (IT) for abusive and criminal purposes. Further, by virtue of the myriad ways in which IT is abused, it represents a technological shift in the nature of crime rather than a new form of criminal behavior. In other words, the nature of crime and its impacts on society are changing to the extent computers and other forms of IT are used for illicit purposes. Understanding the subject, then, is imperative to combatting it and to addressing it at various levels. This work is the first comprehensive encyclopedia to address cybercrime. Topical articles address all key areas of concern and specifically those having to with: terminology, definitions and social constructs of crime; national infrastructure security vulnerabilities and capabilities; types of attacks to computers and information systems; computer abusers and cybercriminals; criminological, sociological, psychological and technological theoretical underpinnings of cybercrime; social and economic impacts of crime enabled with information technology (IT) inclusive of harms experienced by victims of cybercrimes and computer abuse; emerging and controversial issues such as online pornography, the computer hacking subculture and potential negative effects of electronic gaming and so-called computer addiction; bodies and specific examples of U.S. federal laws and regulations that help to prevent cybercrimes; examples and perspectives of law enforcement, regulatory and professional member associations concerned about cybercrime and its impacts; and computer forensics as well as general investigation/prosecution of high tech crimes and attendant challenges within the United States and internationally.

Cyber Crime & Warfare: All That Matters - Peter Warren 2013-07-26

In Cyber Crime: All That Matters, Peter Warren and Michael Streeter outline the history, scale and importance of cyber crime. In particular they show how cyber crime, cyber espionage and cyber warfare now pose a major threat to society. After analysing the origins of computer crime among early hackers the authors describe how criminal gangs and rogue states have since moved into the online arena with devastating effect at a time when the modern world - including all the communication services and utilities we have come to take for granted - has become utterly dependent on computers and the internet.

Cyber Crime - Neil McIntosh 2003

This book identifies cyber crime, explores the arguments made about the seriousness of cyber crime, and discusses what you can do to protect yourself from cyber crime.

Cybercrime and Digital Forensics - Thomas J. Holt 2022-05-30

This book offers a comprehensive and integrative introduction to cybercrime. It provides an authoritative synthesis of the disparate literature on the various types of cybercrime, the global investigation and detection of cybercrime and the role of digital information, and the wider role of technology as a facilitator for social relationships between deviants and criminals. It includes coverage of: • key theoretical and methodological perspectives; • computer hacking and malicious software; • digital piracy and intellectual theft; • economic crime and online fraud; • pornography and online sex crime; • cyber-bullying and cyber-stalking; • cyber-terrorism and extremism; • the rise of the Dark Web; • digital forensic investigation and its legal context around the world; • the law enforcement response to cybercrime transnationally; • cybercrime policy and legislation across the globe. The new edition has been revised and updated, featuring two new chapters; the first offering an expanded discussion of cyberwarfare and information operations online, and the second discussing illicit market operations for all sorts of products on both the Open and Dark Web. This book includes lively and engaging features, such as discussion questions, boxed examples of unique events and key figures in offending, quotes from interviews with active offenders, and a full glossary of terms. It is supplemented by a companion website that includes further exercises for students and instructor resources. This text is essential reading for courses on cybercrime, cyber-deviancy, digital forensics, cybercrime investigation, and the sociology of technology.

Cybercrime: An Encyclopedia of Digital Crime - Nancy E. Marion 2020-10-31

This important reference work is an extensive, up-to-date resource for students wanting to immerse themselves in the world of cybercrime, or for those seeking further knowledge of specific attacks both domestically and internationally. Cybercrime is characterized by criminal acts that take place in the borderless digital realm. It takes on many forms, and its perpetrators and victims are varied. From financial theft, destruction of systems, fraud, corporate espionage, and ransoming of information to the more personal, such as stalking and web-cam spying as well as cyberterrorism, this work covers the full spectrum of crimes committed via cyberspace. This comprehensive encyclopedia covers the most noteworthy attacks while also focusing on the myriad issues that surround cybercrime. It includes entries on such topics as the different types of cyberattacks, cybercrime techniques, specific cybercriminals and cybercrime groups, and cybercrime investigations. While objective in its approach, this book does not shy away from covering such relevant, controversial topics as Julian Assange and Russian interference in the

2016 U.S. presidential election. It also provides detailed information on all of the latest developments in this constantly evolving field. Includes an introductory overview essay that discusses all aspects of cybercrime—how it's defined, how it developed, and its massive expansion in recent years Offers a wide array of entries regarding cybercrime and the many ways it can be committed Explores the largest, most costly cyber attacks on a variety of victims, including corporations, governments, consumers, and individuals Provides up-to-date information on the ever-evolving field of cybercrime

Handbook of Research on Cyber Crime and Information Privacy - Cruz-Cunha, Maria Manuela 2020-08-21

In recent years, industries have transitioned into the digital realm, as companies and organizations are adopting certain forms of technology to assist in information storage and efficient methods of production. This dependence has significantly increased the risk of cyber crime and breaches in data security. Fortunately, research in the area of cyber security and information protection is flourishing; however, it is the responsibility of industry professionals to keep pace with the current trends within this field. The Handbook of Research on Cyber Crime and Information Privacy is a collection of innovative research on the modern methods of crime and misconduct within cyber space. It presents novel solutions to securing and preserving digital information through practical examples and case studies. While highlighting topics including virus detection, surveillance technology, and social networks, this book is ideally designed for cybersecurity professionals, researchers, developers, practitioners, programmers, computer scientists, academicians, security analysts, educators, and students seeking up-to-date research on advanced approaches and developments in cyber security and information protection.

The Deviant Security Practices of Cyber Crime - Erik H.A. van de Sandt 2021-08-09

This is the first book to present a full, socio-technical-legal picture on the security practices of cyber criminals, based on confidential police sources related to some of the world's most serious and organized criminals.

Cyber Crime - John Townsend 2005

Examines different computer crimes, including hacking, computer fraud, viruses, and Internet scams and protection from these crimes.

Cyber Crime Investigator's Field Guide - Bruce Middleton 2022-06-24

Transhumanism, Artificial Intelligence, the Cloud, Robotics, Electromagnetic Fields, Intelligence Communities, Rail Transportation, Open-Source Intelligence (OSINT)—all this and more is discussed in Cyber Crime Investigator’s Field Guide, Third Edition. Many excellent hardware and software products exist to protect our data communications systems, but security threats dictate that they must be all the more enhanced to protect our electronic environment. Many laws, rules, and regulations have been implemented over the past few decades that have provided our law enforcement community and legal system with the teeth needed to take a bite out of cybercrime. But there is still a major need for individuals and professionals who know how to investigate computer network security incidents and can bring them to a proper resolution. Organizations demand experts with both investigative talents and a technical knowledge of how cyberspace really works. The third edition provides the investigative framework that needs to be followed, along with information about how cyberspace works and the tools that reveal the who, where, what, when, why, and how in the investigation of cybercrime. Features New focus area on rail transportation, OSINT, medical devices, and transhumanism / robotics Evidence collection and analysis tools Covers what to do from the time you receive "the call," arrival on site, chain of custody, and more This book offers a valuable Q&A by subject area, an extensive overview of recommended reference materials, and a detailed case study. Appendices highlight attack signatures, Linux commands, Cisco firewall commands, port numbers, and more.

The FBI and Cyber Crime - Robert Grayson 2014-11-17

The federal Bureau of Investigation (FBI) is a national agency dedicated to investigation federal crimes. Founded as a small team of special agents on July 26, 1908, the Bureau was first charged with enforcing the growing body of federal laws covering the United States as a whole. Almost from the beginning of its 100-year history, the Bureau has been the subject of legend and controversy. It has also evolved into a vast and sophisticated national law-enforcement agency. Whether as a federal crime-fighting force or a source of investigative support of local and state police forces, the modern FBI strives to embody its ideals of fidelity, bravery, and integrity. Computers have changed the way people do business, gather information, communicate...and engage in crime. From remote locations in cyber space, criminals can break into a computer and steal valuable information, including credit card and social security numbers, leading to the theft of people's money and identities. Today, the FBI attacks cyber-crime by using sophisticated technology and developing wide-ranging partnerships with companies, academic communities, law enforcement agencies, and concerned individuals-all determined to protect the online community from scam artists, predators, and thieves.

Cyber Crime and Cyber Terrorism - Robert W. Taylor 2018

Revised edition of the authors' Digital crime and digital terrorism, [2015]

Cyber Criminology - K. Jaishankar 2011-02-22

Victimization through the Internet is becoming more prevalent as cyber criminals have developed more effective ways to remain anonymous. And as more personal information than ever is stored on networked computers, even the occasional or non-user is at risk. A collection of contributions from worldwide experts and emerging researchers, Cyber Criminology: Exploring Internet Crimes and Criminal Behavior explores today’s interface of computer science, Internet science, and criminology. Topics discussed include: The growing menace of cyber crime in Nigeria Internet gambling and digital piracy Sexual addiction on the Internet, child pornography, and online exploitation of children Terrorist use of the Internet Cyber stalking and cyber bullying The victimization of women on social networking websites Malware victimization and hacking The Islamic world in cyberspace and the propagation of Islamic ideology via the Internet Human rights concerns that the digital age has created Approaching the topic from a social science perspective, the book explores methods for determining the causes of computer crime victimization by examining an individual’s lifestyle patterns. It also publishes the findings of a study conducted on college students about online victimization. Advances in information and communications technologies have created a range of new crime problems that did not exist two decades ago. Opportunities for various criminal activities to pervade the Internet have led to the growth and development of cyber criminology as a distinct discipline within the criminology framework. This volume explores all aspects of this nascent field and provides a window on the future of Internet crimes and theories behind their origins. K. Jaishankar was the General Chair of the First International Conference of the South Asian Society of Criminology and Victimology (SASCV), held January 15-17, 2011 at the Hotel Jaipur Greens in Jaipur, Rajasthan, India.

Cybercrime - Bernadette Hlubik Schell 2004

Cybercrime: A Reference Handbook documents the history of computer hacking from free long distance phone calls to virtual espionage to worries of a supposed "cyber apocalypse," and provides accessible information everyone should know. An issue so new and evolving so quickly, there are few sources from which readers can get the information they need to inform themselves about and protect themselves from cybercrime. Written by experts in the field, this reference work contains original essays, descriptions of technical aspects, and numerous contributions from over 100 sources. Cybercrime uses fascinating case studies to analyze the beginning of cybercrime and the path it has followed to the present day. With biographical sketches of many influential hackers, the reader will better understand the development of the cybercriminal, and how many of these individuals went on to create some of the computer industry's most useful software. From cyberstalking to viruses, scholars and students alike will find the answers they need to understand these issues. A comprehensive chronology recounting the last four decades of cybercrime, including the implementation and development of legislation and technical attempts to stop further criminal activity An extensive glossary covering criminal, technical, and slang terminology

Blackstone's Handbook of Cyber Crime Investigation - Police National Legal Database (PNLD) 2017

A comprehensive and practical guide to the police investigation of cyber crime offering an overview of the national strategies and structures, a strand-by-strand treatment of the different types of cyber crime, and the relevant laws, police powers, and investigative tools.

Transformational Dimensions of Cyber Crime - Dr M N Sirohi 2015-05-21

Cybercrimes committed against persons include various crimes like transmission of child-pornography harassment of any one with the use of a computer such as email. The trafficking, distribution, posting and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important cybercrimes known today. The worldwide information infrastructure is today increasingly under attack by cyber criminals and terrorists—and the number, cost, and sophistication of the attacks are increasing at alarming rates. The challenge of controlling transnational cyber crime requires a full range of

responses, including both voluntary and legally mandated cooperation This book makes an serious attempt to understand the Cyber Crime which involves activities like Credit Card Frauds, unauthorized excess to other's computer system, Pornography, Software piracy and Cyber stalking etc.

Cyber Crime, Security and Digital Intelligence - Mark Johnson 2016-05-13

Today's digital economy is uniquely dependent on the Internet, yet few users or decision makers have more than a rudimentary understanding of the myriad of online risks that threaten us. Cyber crime is one of the main threats to the integrity and availability of data and systems. From insiders to complex external attacks and industrial worms, modern business faces unprecedented challenges; and while cyber security and digital intelligence are the necessary responses to this challenge, they are understood by only a tiny minority. In his second book on high-tech risks, Mark Johnson goes far beyond enumerating past cases and summarising legal or regulatory requirements. He describes in plain, non-technical language how cyber crime has evolved and the nature of the very latest threats. He confronts issues that are not addressed by codified rules and practice guidelines, supporting this with over 30 valuable illustrations and tables. Written for the non-technical layman and the high tech risk manager alike, the book also explores countermeasures, penetration testing, best practice principles, cyber conflict and future challenges. A discussion of Web 2.0 risks delves into the very real questions facing policy makers, along with the pros and cons of open source data. In a chapter on Digital Intelligence readers are provided with an exhaustive guide to practical, effective and ethical online investigations. Cyber Crime, Security and Digital Intelligence is an important work of great relevance in today's interconnected world and one that nobody with an interest in either risk or technology should be without.

Cybercrime - Susan W. Brenner 2010

Enhancing her narrative with real-life stories, the author traces the rise of cybercrime from mainframe computer hacking in the 1950s to the organized, professional, and often transnational cybercrime that has become the norm in the 21st century.

Cybercrime - Noah Berlatsky 2013-10-11

This concise volume takes care of two major issues at once; providing readers with a more worldwide view than American-centric information, and educating readers about cybercrime. This volume of essays from international sources explores the vulnerability of countries and people to cybercrime. Readers will explore cybercrime law worldwide, and take a look at the role of organized crime in cybercrime. They will also take a deep dive into cyber espionage and cyber terrorism. Countries and cultures that readers will learn about include South Africa, Singapore, Pakistan, China, Canada, Thailand, Australia, Russia, and the United Kingdom.