Online Library Computer Forensics And Cyber Crime Mabisa Pdf Free Copy

Computer Forensics and Cyber Crime Principles of Cybercrime Handbook of Research on Cyber Crime and Information Privacy Cyber Crime and Cyber Terrorism Hunting Cyber Criminals Transformational Dimensions of Cyber Crime Cybercrime Cyber Crime and Digital Disorder Cyber Crime & Warfare: All That Matters Cybercrime Investigators Handbook Cybercrime Cyber Crime and Cyber Terrorism Investigator's Handbook Digital Evidence and Computer Crime Cyber Crime: Concepts, Methodologies, Tools and Applications Cybercrime and Digital Forensics Cybercrime and the Law Digital Evidence and Computer Crime The FBI and Cyber Crime Crime and the Internet Digital Forensics and Cyber Crime Cybercrime Cybercrime and Its Victims Cybercrime The Transnational Dimension of Cyber Crime and Terrorism The Psychology of Cyber Crime: Concepts and Principles Policing Cyber Hate, Cyber Threats and Cyber Terrorism The Deviant Security Practices of Cyber Crime Cyber Crime Cyber Economic Crime in India Cyber Crime The Elite Cyber Criminals' Stories The Human Factor of Cybercrime Cybercrime and Cybersecurity in the Global South Cyber Crime An Overview on Cybercrime & Security, Volume - I Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives Cyber Crime Digital Crime Investigation Artificial Intelligence and the Law Cyber Criminology

The Psychology of Cyber Crime: Concepts and Principles Jul 27 2021 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.

Artificial Intelligence and the Law May 13 2020 This volume presents new research in artificial intelligence (AI) and Law with special reference to criminal justice. It brings together leading international experts including computer scientists, lawyers, judges and cyber-psychologists. The book examines some of the core problems that technology raises for criminal law ranging from privacy and data protection, to cyber-warfare, through to the theft of virtual property. Focusing on the West and China, the work considers the issue of AI and the Law in a comparative context presenting the research from a cross-jurisdictional and cross-disciplinary approach. As China becomes a global leader in AI and technology, the book provides an essential in-depth understanding of domestic laws in both Western jurisdictions and China on criminal liability for cybercrime. As such, it will be a valuable resource for academics and researchers working in the areas of AI, technology and criminal justice.

The Elite Cyber Criminals' Stories Jan 21 2021 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.

Cybercrime Oct 10 2022 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.

The FBI and Cyber Crime Mar 03 2022 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.

Computer Forensics and Cyber Crime Aug 20 2023 This work defines cyber crime, introduces students to computer terminology and the history of computer crime, and includes discussions of important legal and social issues relating to computer crime. The text also covers computer forensic science.

Hunting Cyber Criminals Apr 16 2023 The skills and tools for collecting, verifying and correlating information from different types of systems is an essential skill when tracking down hackers. This book explores Open Source Intelligence Gathering (OSINT) inside out from multiple perspectives, including those of hackers and seasoned intelligence experts. OSINT refers to the techniques and tools required to harvest publicly available data concerning a person or an organization. With several years of experience of tracking hackers with OSINT, the author whips up a classical plot-line involving a hunt for a threat actor. While taking the audience through the thrilling investigative drama, the author immerses the audience with in-depth knowledge of state-of-the-art OSINT tools and techniques. Technical users will want a basic understanding of the Linux command line in order to follow the examples. But a person with no Linux or programming experience can still gain a lot from this book through the commentaries. This book's unique digital investigation proposition is a combination of story-telling, tutorials, and case studies. The book explores digital investigation from multiple angles: Through the eyes of the author who has several years of experience in the subject. Through the mind of the hacker who collects massive amounts of data from multiple online sources to identify targets as well as ways to hit the targets. Through the eyes of industry leaders. This book is ideal for: Investigation professionals, forensic analysts,

and CISO/CIO and other executives wanting to understand the mindset of a hacker and how seemingly harmless information can be used to target their organization. Security analysts, forensic investigators, and SOC teams looking for new approaches on digital investigations from the perspective of collecting and parsing publicly available information. CISOs and defense teams will find this book useful because it takes the perspective of infiltrating an organization from the mindset of a hacker. The commentary provided by outside experts will also provide them with ideas to further protect their organization's data.

Cyber Crime: Concepts, Methodologies, Tools and Applications Jul 07 2022 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 Jul 15 2020 A new and terrifying dimension of the electronic age, cyber-crime is flourishing with no regard for national boundaries. This constantly evolving global phenomenon leaves law enforcement struggling to catch up. The culture of the Internet has led young people to idolize computer hackers and sometimes commit criminal acts. The motive of virus writers varies and organized crime has even gotten in on the action. The largely unchecked spread of cyber-crime has led to the creation of a global force to combat it. There are many losers in this dangerous game, and the stakes could not be higher. Each title in this series contains a foreword from the Chairman of the National Law

Enforcement Association, color photos throughout, charts, and back matter including: an index, chronology, and further reading lists for books and internet resources. Key Icons appear throughout the books in this series in an effort to encourage library readers to build knowledge, gain awareness, explore possibilities and expand their viewpoints through our content rich non-fiction books. Key Icons in this series are as follows: Words to Understand are shown at the front of each chapter with definitions. These words are set in boldfaced type in that chapter, so that readers are able to reference back to the definitions--building their vocabulary and enhancing their reading comprehension. Sidebars are highlighted graphics with content rich material within that allows readers to build knowledge and broaden their perspectives by weaving together additional information to provide realistic and holistic perspectives. Text-Dependent Questions are placed at the end of each chapter. They challenge the reader's comprehension of the chapter they have just read, while sending the reader back to the text for more careful attention to the evidence presented there. Research Projects are provided at the end of each chapter as well and provide readers with suggestions for projects that encourage deeper research and analysis. And a Series Glossary of Key Terms is included in the back matter containing terminology used throughout the series. Words found here broaden the reader's knowledge and understanding of terms used in this field.

Digital Evidence and Computer Crime Aug 08 2022 Digital evidence--evidence that is stored on or transmitted by computers--can play a major role in a wide range of crimes, including homicide, rape, abduction, child abuse, solicitation of minors, child pornography, stalking, harassment, fraud, theft, drug trafficking, computer intrusions, espionage, and terrorism. Though an increasing number of criminals are using computers and computer networks, few investigators are well-versed in the evidentiary, technical, and legal issues related to digital evidence. As a result, digital evidence is often overlooked, collected incorrectly, and analyzed ineffectively. The aim

of this hands-on resource is to educate students and professionals in the law enforcement, forensic science, computer security, and legal communities about digital evidence and computer crime. This work explains how computers and networks function, how they can be involved in crimes, and how they can be used as a source of evidence. As well as gaining a practical understanding of how computers and networks function and how they can be used as evidence of a crime, readers will learn about relevant legal issues and will be introduced to deductive criminal profiling, a systematic approach to focusing an investigation and understanding criminal motivations.

Cybercrime and Cybersecurity in the Global South Nov 18 2020 Integrating theories from a wide range of disciplines, Nir Kshetri compares the patterns, characteristics and processes of cybercrime activities in major regions and economies in the Global South such as China, India, the former Second World economies, Latin America and the Caribbean, Sub-Saharan Africa and Middle East and North Africa.

Cybercrime Nov 30 2021 As technology develops and internet-enabled devices become ever more prevalent new opportunities exist for that technology to be exploited by criminals. One result of this is that cybercrime is increasingly recognised as a distinct branch of criminal law. This book is designed for students studying cybercrime for the first time, enabling them to get to grips with an area of rapid change. The book offers a thematic and critical overview of cybercrime, introducing the key principles and clearly showing the connections between topics as well as highlighting areas subject to debate. Written with an emphasis on the law in the UK but considering in detail the Council of Europe's important Convention on Cybercrime, this text also covers the jurisdictional aspects of cybercrime in international law. Themes discussed include crimes against computers, property, offensive content, and offences against the person, and recent controversial areas such as cyberterrorism and cyber-harassment are explored. Clear, concise and critical, this text offers a valuable overview

of this fast-paced and growing area of law.

Handbook of Research on Cyber Crime and Information Privacy Jun 18 2023 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.

Cybercrime and Its Victims Oct 30 2021 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.

Cyber Crime and Cyber Terrorism May 17 2023 Revised edition of the authors' Digital crime and digital terrorism, [2015]

Cybercrime Feb 14 2023 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.

Cybercrime and Digital Forensics Jun 06 2022 The emergence of the World Wide Web, smartphones, and Computer-Mediated Communications (CMCs) profoundly affect the way in which people interact online and offline. Individuals who engage in socially unacceptable or outright criminal acts increasingly utilize technology to connect with one another in ways that are not otherwise possible in the real world due to shame, social stigma, or risk of detection. As a

consequence, there are now myriad opportunities for wrongdoing and abuse through technology. This book offers a comprehensive and integrative introduction to cybercrime. It is the first to connect the disparate literature on the various types of cybercrime, the 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 digital piracy, economic crime and online fraud, pornography and online sex crime, cyber-bulling and cyber-stalking, cyber-terrorism and extremism, digital forensic investigation and its legal context, cybercrime policy. 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 students exercises and instructor resources. This text is essential reading for courses on cybercrime, cyber-deviancy, digital forensics, cybercrime investigation and the sociology of technology.

Cyber Economic Crime in India Mar 23 2021 This volume provides an overview of cyber economic crime in India, analyzing fifteen years of data and specific case studies from Mumbai to add to the limited research in cyber economic crime detection. Centering around an integrated victim-centered approach to investigating a global crime on the local level, the book examines the criminal justice system response to cyber economic crime and proposes new methods of detection and prevention. It considers the threat from a national security perspective, a cybercrime perspective, and as a technical threat to business and technology installations. Among the topics discussed: Changing landscape of crime in cyberspace Cybercrime typology Legal framework for cyber economic crime in India Cyber security mechanisms in India A valuable resource for law enforcement and police working on the local, national, and global level in the detection and prevention of cybercrime, Cyber

Economic Crime in India will also be of interest to researchers and practitioners working in financial crimes and white collar crime.

An Overview on Cybercrime & Security, Volume - I Sep 16 2020 Cybersecurity is significant in light of the fact that cybersecurity chance is expanding. Driven by worldwide network and use of cloud administrations, similar to Amazon Web Services, to store touchy information and individual data. Across the board, helpless setup of cloud administrations combined with progressively refined cybercriminals implies the hazard that your association experiences a fruitful digital assault or information break is on the ascent. Digital dangers can emerge out of any degree of your association. You should teach your staff about basic social building tricks like phishing and more complex cybersecurity assaults like ransomware or other malware intended to take protected innovation or individual information and many more. I hereby present a manual which will not only help you to know your rights as well as how to keep yourself safe on cyberspace. The book has been awarded by many experts as well as it has also been recognised by the University of Mumbai for their B.com - Banking & Insurance as well as on Investment Management Program.

Policing Cyber Hate, Cyber Threats and Cyber Terrorism Jun 25 2021 What are cyber threats? This book brings together a diverse range of multidisciplinary ideas to explore the extent of cyber threats, cyber hate and cyber terrorism. This ground-breaking text provides a comprehensive understanding of the range of activities that can be defined as cyber threats. It also shows how this activity forms in our communities and what can be done to try to prevent individuals from becoming cyber terrorists. This text will be of interest to academics, professionals and practitioners involved in building social capital; engaging with hard to reach individuals and communities; the police and criminal justice sector as well as IT professionals.

Cyber Crime and Cyber Terrorism Investigator's Handbook Sep 09 2022 Cyber Crime and Cyber Terrorism Investigator's Handbook is a vital tool in the arsenal of today's computer

programmers, students, and investigators. As computer networks become ubiquitous throughout the world, cyber crime, cyber terrorism, and cyber war have become some of the most concerning topics in today's security landscape. News stories about Stuxnet and PRISM have brought these activities into the public eye, and serve to show just how effective, controversial, and worrying these tactics can become. Cyber Crime and Cyber Terrorism Investigator's Handbook describes and analyzes many of the motivations, tools, and tactics behind cyber attacks and the defenses against them. With this book, you will learn about the technological and logistic framework of cyber crime, as well as the social and legal backgrounds of its prosecution and investigation. Whether you are a law enforcement professional, an IT specialist, a researcher, or a student, you will find valuable insight into the world of cyber crime and cyber warfare. Edited by experts in computer security, cyber investigations, and counter-terrorism, and with contributions from computer researchers, legal experts, and law enforcement professionals, Cyber Crime and Cyber Terrorism Investigator's Handbook will serve as your best reference to the modern world of cyber crime. Written by experts in cyber crime, digital investigations, and counter-terrorism Learn the motivations, tools, and tactics used by cyber-attackers, computer security professionals, and investigators Keep up to date on current national and international law regarding cyber crime and cyber terrorism See just how significant cyber crime has become, and how important cyber law enforcement is in the modern world

Cybercrime and the Law May 05 2022 The first full-scale overview of cybercrime, law, and policy

Transformational Dimensions of Cyber Crime Mar 15 2023 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.

Digital Crime Investigation Jun 13 2020 "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.

Cybercrime Sep 28 2021 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.

Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives Aug 16 2020 Recent developments in cyber security, crime, and forensics have attracted researcher and practitioner interests from technological, organizational and policy-making perspectives. Technological advances address challenges in information sharing, surveillance and analysis, but organizational advances are needed to foster collaboration between federal, state and local agencies as well as the private sector. Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives provides broad coverage of technical and socio-economic perspectives for utilizing information and communication technologies and developing practical solutions in cyber security, cyber crime and cyber forensics.

Digital Evidence and Computer Crime Apr 04 2022 Though an increasing number of criminals are using computers and computer networks, few investigators are well versed in the issues related to digital evidence. This work explains how computer networks function and how they can be used in a crime.

Cyber Crime Oct 18 2020 Examines different computer crimes, including hacking, computer fraud, viruses, and Internet scams and protection from these crimes.

Cybercrime Investigators Handbook Nov 11 2022 The investigator's practical guide for cybercrime evidence identification and collection Cyber attacks perpetrated against businesses, governments, organizations, and individuals have been occurring for decades. Many attacks are discovered only after the data has been exploited or sold on the criminal markets. Cyber attacks damage both the finances and reputations of businesses and cause damage to the ultimate victims of the crime. From the perspective of the criminal, the current state of inconsistent security policies and lax investigative procedures is a profitable

and low-risk opportunity for cyber attacks. They can cause immense harm to individuals or businesses online and make large sums of money—safe in the knowledge that the victim will rarely report the matter to the police. For those tasked with probing such crimes in the field, information on investigative methodology is scarce. The Cybercrime Investigators Handbook is an innovative guide that approaches cybercrime investigation from the field-practitioner's perspective. While there are high-quality manuals for conducting digital examinations on a device or network that has been hacked, the Cybercrime Investigators Handbook is the first guide on how to commence an investigation from the location the offence occurred—the scene of the cybercrime—and collect the evidence necessary to locate and prosecute the offender. This valuable contribution to the field teaches readers to locate, lawfully seize, preserve, examine, interpret, and manage the technical evidence that is vital for effective cybercrime investigation. Fills the need for a field manual for front-line cybercrime investigators Provides practical guidance with clear, easy-to-understand language Approaches cybercrime form the perspective of the field practitioner Helps companies comply with new GDPR guidelines Offers expert advice from a law enforcement professional who specializes in cybercrime investigation and IT security Cybercrime Investigators Handbook is much-needed resource for law enforcement and cybercrime investigators, CFOs, IT auditors, fraud investigators, and other practitioners in related areas.

Cyber Criminology Apr 11 2020 This book provides a comprehensive overview of the current and emerging challenges of cyber criminology, victimization and profiling. It is a compilation of the outcomes of the collaboration between researchers and practitioners in the cyber criminology field, IT law and security field. As Governments, corporations, security firms, and individuals look to tomorrow's cyber security challenges, this book provides a reference point for experts and forward-thinking analysts at a time when the debate over how we plan for the

cyber-security of the future has become a major concern. Many criminological perspectives define crime in terms of social, cultural and material characteristics, and view crimes as taking place at a specific geographic location. This definition has allowed crime to be characterised, and crime prevention, mapping and measurement methods to be tailored to specific target audiences. However, this characterisation cannot be carried over to cybercrime, because the environment in which such crime is committed cannot be pinpointed to a geographical location, or distinctive social or cultural groups. Due to the rapid changes in technology, cyber criminals' behaviour has become dynamic, making it necessary to reclassify the typology being currently used. Essentially, cyber criminals' behaviour is evolving over time as they learn from their actions and others' experiences, and enhance their skills. The offender signature, which is a repetitive ritualistic behaviour that offenders often display at the crime scene, provides law enforcement agencies an appropriate profiling tool and offers investigators the opportunity to understand the motivations that perpetrate such crimes. This has helped researchers classify the type of perpetrator being sought. This book offers readers insights into the psychology of cyber criminals, and understanding and analysing their motives and the methodologies they adopt. With an understanding of these motives, researchers, governments and practitioners can take effective measures to tackle cybercrime and reduce victimization.

Principles of Cybercrime Jul 19 2023 A comprehensive doctrinal analysis of cybercrime laws in four major common law jurisdictions: Australia, Canada, the UK and the US.

The Human Factor of Cybercrime Dec 20 2020 Cybercrimes are often viewed as technical offenses that require technical solutions, such as antivirus programs or automated intrusion detection tools. However, these crimes are committed by individuals or networks of people which prey upon human victims and are detected and prosecuted by criminal justice personnel. As a result, human decision-making plays a substantial role in the course of an offence, the justice

response, and policymakers' attempts to legislate against these crimes. This book focuses on the human factor in cybercrime: its offenders, victims, and parties involved in tackling cybercrime. The distinct nature of cybercrime has consequences for the entire spectrum of crime and raises myriad questions about the nature of offending and victimization. For example, are cybercriminals the same as traditional offenders, or are there new offender types with distinct characteristics and motives? What foreground and situational characteristics influence the decision-making process of offenders? Which personal and situational characteristics provide an increased or decreased risk of cybercrime victimization? This book brings together leading criminologists from around the world to consider these questions and examine all facets of victimization, offending, offender networks, and policy responses. Chapter 13 of this book is freely available as a downloadable Open Access PDF at http://www.taylorfrancis.com under a Creative Commons Attribution-Non Commercial-No Derivatives (CC-BY-NC-ND) 4.0 license.

Digital Forensics and Cyber Crime Jan 01 2022 This book constitutes the thoroughly refereed post-conference proceedings of the 5th International ICST Conference on Digital Forensics and Cyber Crime, ICDF2C 2013, held in September 2013 in Moscow, Russia. The 16 revised full papers presented together with 2 extended abstracts and 1 poster paper were carefully reviewed and selected from 38 submissions. The papers cover diverse topics in the field of digital forensics and cybercrime, ranging from regulation of social networks to file carving, as well as technical issues, information warfare, cyber terrorism, critical infrastructure protection, standards, certification, accreditation, automation and digital forensics in the cloud.

Cyber Crime and Digital Disorder Jan 13 2023

Cyber Crime & Warfare: All That Matters Dec 12 2022 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.

The Transnational Dimension of Cyber Crime and Terrorism Aug 28 2021 In December 1999, more than forty members of government, industry, and academia assembled at the Hoover Institution to discuss this problem and explore possible countermeasures. The Transnational Dimension of Cyber Crime and Terrorism summarizes the conference papers and exchanges, addressing pertinent issues in chapters that include a review of the legal initiatives undertaken around the world to combat cyber crime, an exploration of the threat to civil aviation, analysis of the constitutional, legal, economic, and ethical constraints on use of technology to control cyber crime, a discussion of the ways we can achieve security objectives through international cooperation, and more. Much has been said about the threat posed by worldwide cyber crime, but little has been done to protect against it. A transnational response sufficient to meet this challenge is an immediate and compelling necessity—and this book is a critical first step in that direction.

Cyber Crime Feb 19 2021 Cyber Crime, Second Edition by Catherine D. Marcum, 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 Second Edition: A new chapter explores the many forms of nonconsensual pornography—doxxing, downblousing, upskirting, revenge porn, sextortion—and its negative effects on victims and society. New features—Key Words, Questions to Consider While Reading, and end-of-chapter Discussion Question—help students focus on key concepts. Discussions of the latest issues—the Convention on Cybercrime, R.B. Cialdini's research into grooming, neutralization (or rationalization) of behaviors, transaction laundering, and cyber dating—keep students current with recent developments. Updates include the latest statistics from the National Center for Missing and Exploited Children, case studies with recent developments and rulings (Playpen, Tor), and expanded coverage of online prostitution and Internet safety for minors. 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 A range of theories and perspectives that shed light on the complexity of Internet-based crime 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 cyber crime Coverage of the most widespread and damaging types of cyber crime intellectual property theft online sexual victimization identity theft cyber fraud and financial crimes harassment

Crime and the Internet Feb 02 2022 This groundbreaking text examines for the first time the nature and consequences of crime on the internet, and analyses the new challenges that cybercrimes pose to the criminal justice system.

Cyber Crime Apr 23 2021 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.

The Deviant Security Practices of Cyber Crime May 25 2021 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.