Cybercrime And Digital Deviance

BAKER KANE

Industry of Anonymity Taylor & Francis
Updated to include the most current events and information on cyberterrorism, the second edition of Computer Forensics: Cybercriminals, Laws, and Evidence continues to balance technicality and legal analysis as it enters into the world of cybercrime by exploring what it is, how it is investigated, and the regulatory laws around the collection and use of electronic evidence. Students are introduced to the technology involved in computer forensic investigations and the technical and legal difficulties involved in searching, extracting, maintaining, and storing electronic evidence, while simultaneously looking at the legal implications of such investigations and the rules of legal procedure relevant to electronic evidence. Significant and current computer forensic developments are examined, as well as the implications for a variety of fields including computer science, security, criminology, law, public policy, and administration.
Researching Cybercrimes Routledge
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.
Computer Forensics and Digital Investigation with EnCase Forensic v7 Routledge
The authors are proud sponsors of the 2020 SAGE Keith Roberts Teaching Innovations Award—enabling graduate students and early career faculty to attend the annual ASA pre-conference teaching and learning workshop. "Very practical approach to teaching research methods and very student friendly. This text "breathes life" into the research process. —Sherill Morris-Francis, Mississippi Valley State University The Practice of Research in Criminology and Criminal Justice, Seventh Edition demonstrates the vital role research plays in criminology and criminal justice by integrating in-depth, real-world case studies with a comprehensive discussion of research methods. By pairing research techniques with practical examples from the field, Ronet D. Bachman and Russell K. Schutt equip students to critically evaluate and confidently conduct research. The Seventh Edition of this best-selling text retains the strengths of previous editions while breaking ground with emergent research methods, enhanced tools for learning in the text and online, and contemporary, fascinating research findings. This edition incorporates new topics like intelligence-led policing, social network analysis (SNA), the evolution of cybercrime, and more. Students engage with the wide realm of research methods available to them, delve deeper into topics relevant to their field of study, and benefit from the wide variety of new exercises to help them practice as they learn. Give your students the SAGE edge! SAGE edge offers a robust online environment featuring an impressive array of free tools and resources for review, study, and further exploration, keeping both instructors and students on the cutting edge of teaching and learning.
Cybercrime and Digital Deviance Springer
Cybercrime is a complex and ever-changing phenomenon. This book offers a clear and engaging introduction to this fascinating subject by situating it in the wider context of social, political, cultural and economic change. Taking into account recent developments in social networking and mobile communications, this new edition tackles a range of themes spanning criminology, sociology, law, politics and cultural studies, including: - computer hacking - cyber-terrorism - piracy and intellectual property theft - financial fraud and identity theft - hate speech - internet pornography - online stalking - policing the internet - surveillance and censorship Complete with useful recommendations for further reading, incisive discussion questions and an updated glossary of key terms, Cybercrime and Society is an essential resource for all students and academics interested in cybercrime and the future of the Internet.

Dot.cons Springer Nature
An essential reference for scholars and others whose work brings them into contact with managing, policing and regulating online behaviour, the Handbook of Internet Crime emerges at a time of rapid social and technological change. Amidst much debate about the dangers presented by the Internet and intensive negotiation over its legitimate uses and regulation, this is the most comprehensive and ambitious book on cybercrime to date. The Handbook of Internet Crime gathers together the leading scholars in the field to explore issues and debates surrounding internet-related crime, deviance, policing, law and regulation in the 21st century. The Handbook reflects the range and depth of cybercrime research and scholarship, combining contributions from many of those who have established and developed cyber research over the past 25 years and who continue to shape it in its current phase, with more recent entrants to the field who are building on this tradition and breaking new ground. Contributions reflect both the global nature of cybercrime problems, and the international span of scholarship addressing its challenges.
Cybercrime in Context Springer Nature
A unique and comprehensive overview of the field and its current issues, Cybercriminology analyzes cybercrimes through the lens of criminology. Featuring an accessible, conversational writing style, it first discusses traditional criminological theories of criminal behavior and then analyzes how these theories--the existing literature and empirical studies--can be applied to explain cybercrimes. The text also introduces students to types of cybercrime, the nature and extent of cybercrime in the U.S. and abroad, and victim and offender behavior in the online environment. FEATURES * Real-world case studies and examples demonstrate the extent and complexity of cybercriminology * Boxed features present compelling research topics and scenarios * Review questions stimulate classroom discussions * An Ancillary Resource Center contains an Instructor's Manual, a Test Bank, and PowerPoint lecture outlines
Cybercrime and Society Routledge
Computers and the Internet play an increasingly pivotal role in daily life, making it vitally important to understand the dynamics of cybercrime and those victimized by it. The anthology Cybercrime and Criminological Theory: Fundamental Readings on Hacking, Piracy, Theft, and Harassment explores the predictors for participation in various forms of cybercrime and deviance, from common problems like media piracy, to more distinct offenses such as computer hacking. Most criminological theories were developed to account for street crimes, so it is unclear how these theories may apply to virtual offending. This text provides critical insight into the utility of multiple theories to account for cybercrimes. Cybercrime and Criminological Theory gives direct insight into the rates and prevalence of cybercrime offenses using data sets from populations across the United States. It gives readers a fundamental understanding of, and appreciation for various forms of cybercrime, and outlines prospective predictors of both offending and victimization. The selected readings identify research questions that must be addressed in order to improve the legal, technical, and policy responses to cybercrimes. Cybercrime and Criminological Theory begins with an introduction to cybercrime and virtual criminality. From there, the book offers five sections featuring seminal and cutting edge works on topics in: - Routine Activities Theory - Deterrence Theory - Social Learning and Self Control - General Strain Theory - Deviant Subcultures The book uses articles and cutting-edge research in the field to create a text that is relevant for students at all levels of study, as well as scholars in criminology, sociology, and information security. Undergraduate students will gain insight into the value of various theories to account for victimization and offending, and learn basic research methods applied by criminologists to assess crime and victimization. Graduate students benefit from the detail provided on research methods, measurement, and research questions that must be addressed to fully understand cybercrimes. Thomas J. Holt earned his Ph.D. at the University of Missouri, Saint Louis. He is currently an Associate Professor in the School of Criminal

Justice at Michigan State University. His areas of research include computer hacking, malware, and the role played by technology and computer-mediated communications in facilitating crime and deviance. Dr. Holt is the co-author of Digital Crime and Digital Terror, and the co-editor of Corporate Hacking and Technology-Driven Crime. He is also the editor of the book Cybercrime: Causes, Correlates, and Context. His work has also been published in numerous academic journals, including Crime and Delinquency, Deviant Behavior, and the Journal of Criminal Justice. Dr. Holt received two grants from the U.S. National Institute of Justice to examine the market for malicious software, and the social dynamics of carders and on-line data thieves. Additionally, he is the project lead for the Spartan Devils Chapter of the Honeynet Project, and directs the MSU Open Source Research Laboratory, which explores cyber threats around the globe through on-line research.

Online Othering SAGE Publications

This book articulates how crime prevention research and practice can be reimagined for an increasingly digital world. This ground-breaking work explores how criminology can apply longstanding, traditional crime prevention techniques to the digital realm. It provides an overview of the key principles, concepts and research literature associated with crime prevention, and discusses the interventions most commonly applied to crime problems. The authors review the theoretical underpinnings of these and analyses evidence for their efficacy. Cybercrime Prevention is split into three sections which examine primary prevention, secondary prevention and tertiary prevention. It provides a thorough discussion of what works and what does not, and offers a formulaic account of how traditional crime prevention interventions can be reimagined to apply to the digital realm.

Cybercrime and Digital Forensics Jones & Bartlett Publishers

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 Digital Forensics World Scientific

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.

Crime On-line Oxford Handbooks

"In light of the increasing adoption of technology, it is critical that researchers explore the complex effects of computer technology on human behavior and the intersection of real world and virtual experiences. Crime Online uses empirical tests and unique data to provide detailed criminological explorations of multiple forms of cybercrime, including phishing, hacking, and sex crimes. This text also includes a comprehensive exploration of cyberterrorism and activism in online environments. The law enforcement and policy responses to cybercrimes at the local, state, and federal level are also discussed in detail. This work provides practical policy discussions that will benefit academics, law enforcement, legal counsel, and students at the undergraduate and graduate level"--

The Digital Practices of African Americans Bloomsbury Publishing USA

This initiating monograph provides the first thorough examination of the concept of white-collar crime online. Applying an offender-based perspective which considers the central role of convenience, it seeks to inform, improve and develop the current literature on cybercrime, whilst paying particular attention to its founding category within criminology. It argues that white-collar crime has receded from criminological perspectives on cybercrime in recent years and that a detailed, rich re-assessment of white-collar crime in contemporary digital societies is needed. Following a theoretical introduction, the book develops to discuss, inter alia, implications for corporate reputation, the various organizational roles utilized in mitigating external and internal threats, the unique considerations involved in law enforcement efforts, and likely future directions within the field. White-Collar Crime Online recognises the strong lineage and correlation that exists between the study of white-collar crime and cybercrime. Using convenience theory within a comparative analysis which includes case-studies, the book explores both European and American paradigms, perspectives and models to determine where white-collar crime exists within the contemporary workplace and how this might relate to the ongoing discourse on cybercrime. In doing so it revaluates criminological theory within the context of changing patterns of business, the workplace, social rules, systems of governance, decision making, social ordering and control. White-Collar Crime Online will speak to criminologists, sociologists and professionals; including those interested in cyber-security, economics, technology and computer science.

Digital Criminology Springer Science & Business Media

This exciting and timely collection showcases recent work on Cybercrime by members of Uclan Cybercrime Research Unit [UCRU], directed by Dr Tim Owen at the University of Central Lancashire, UK. This book offers up-to-date perspectives on Cybercrime based upon a Realist social ontology, alongside suggestions for how research into Cybercrime might move beyond what can be seen as the main theoretical obstacles facing criminological theory: the stagnation of critical criminology and the nihilistic relativism of the postmodern and post-structuralist cultural turn. Organised into three sections; 'Law and Order in Cyberspace', 'Gender and Deviance in Cyberspace', and 'Identity and Cyberspace', this cutting-edge volume explores some of the most crucial issues we face today on the internet: grooming, gendered violence, freedom of speech and intellectual property crime. Providing unique new theory on Cybercrime, this book will appeal to scholars and advanced students of Criminology, Law, Sociology, Philosophy, Policing and Forensic Science, Information Technology and Journalism, in addition to professionals working within law and order agencies and the security services.

Cybercrime Prevention Springer Nature

Amidst the sensationalist claims about the dangers of the Internet, Virtually Criminal provides an empirically grounded criminological analysis of deviance and regulation within an online community. It integrates theory and empiricism to forge an explanation of cybercrime whilst offering new insights into online regulation. One of the first studies to further our understanding of the causes of cyber deviance, crime and its control, this groundbreaking study from Matthew Williams takes the Internet as a site of social and cultural (re)production, and acknowledges the importance of online social/cultural formations in the genesis and regulation of cyber deviance and crime. A blend of criminological, sociological and linguistic theory, this book provides a unique understanding of the aetiology of cybercrime and deviance. Focus group and offence data are analyzed and an interrelationship between online community, deviance and regulation is established. The subject matter of the book is inherently transnational. It makes extensive use of a number of international case studies, ensuring it is relevant to readers in multiple countries (especially the US, the UK and Australasia). Pioneering and innovative, this fascinating book will be of interest to students and researchers across the disciplines of sociology, criminology, law and media and communication studies.

Media and Crime Springer

A comprehensive and state-of the-art overview from internationally-recognized experts on white-collar crime covering a broad range of topics from many perspectives Law enforcement professionals and criminal justice scholars have debated the most appropriate definition of "white-collar crime" ever since Edwin Sutherland first coined the phrase in his speech to the American Sociological Society in 1939. The conceptual ambiguity surrounding the term has challenged efforts to construct a body of science that meaningfully informs policy and theory. The Handbook of White-Collar Crime is a unique re-framing of traditional discussions that discusses common topics of white-collar crime—who the offenders are, who the victims are, how these crimes are punished, theoretical explanations—while exploring how the choice of one definition over another affects research and scholarship on the subject. Providing a one-volume overview of research on white-collar crime, this book presents diverse perspectives from an international team of both established and newer scholars that review theory, policy, and empirical work on a broad range of topics. Chapters explore the extent and cost of white-collar crimes, individual- as well as organizational- and macro-level theories of crime, law enforcement roles in prevention and intervention, crimes in Africa and South America, the influence of technology and globalization, and more. This important resource: Explores diverse implications for future theory, policy, and research on current and emerging issues in the field Clarifies distinct characteristics of specific types of offences within the general archetype of white-collar crime Includes chapters written by researchers from countries commonly underrepresented in the field Examines the real-world impact of ambiguous definitions of white-collar crime on prevention, investigation, and punishment Offers critical examination of how definitional decisions steer the direction of criminological scholarship Accessible to readers at the undergraduate level, yet equally relevant for experienced practitioners, academics, and researchers, The Handbook of White-Collar Crime is an innovative, substantial contribution to contemporary scholarship in the field.

Cybercrime Oxford University Press, USA

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 Criminology Springer

This book is about the human factor in cybercrime: its offenders, victims and parties involved in tackling cybercrime. It takes a diverse international perspective of the response to and prevention of cybercrime by seeking to understand not just the technological, but the human decision-making involved. This edited volume represents the state of the art of research on the human factor in cybercrime, addressing its victims, offenders, and policing. It originated at the Second annual Conference on the Human Factor in Cybercrime, held in The Netherlands in October 2019, bringing together empirical research from a variety of disciplines, and theoretical and methodological approaches. This volume will be of particular interest to researchers and students in cybercrime and the psychology of cybercrime, as well as policy makers and law enforcement interested in prevention and detection.

Crime and the Internet SAGE Publications

"This book addresses various aspects of hacking and technology-driven crime, including the ability to understand computer-based threats, identify and examine attack dynamics, and find solutions"--Provided by publisher.

The Handbook of White-Collar Crime Routledge

This book crosses the boundaries of sociological, criminological and cultural discourse in order to explore the implications of recent massive transformations in information and communication technologies for the growth of criminal and deviant identities and behaviour on the Internet.

Cybercriminology Routledge

This handbook offers a comprehensive examination of crimes as public policy subjects to provide an authoritative overview of current knowledge about the nature, scale, and effects of diverse forms of criminal behaviour and of efforts to prevent and control them.