Mafiaboy

Countering Terrorism
Confessions of Teenage Hackers
UNB Law Journal
Cybersecurity Breaches and Issues Surrounding Online Threat Protection
Management Information Systems
Cybercrime and the Law
Cyber Crimes
When Technocultures Collide
Crime, Conflict and Security in Cyberspace
Managing Information Technology in the Business Enterprise
A History of Cyber Security Attacks
America's Battle Against Russia, China, and the Rising Global Cyber Threat
A Reference Handbook
Computers and Society
Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications
Dawn of the Code War
The Emerging Fault Lines of the Nation State
Computer Investigation
Cyber Crime: Concepts, Methodologies, Tools and Applications
Greed, Corruption, Villains, and Victims
Modern Perspectives
Cyber Crime and Cyber Terrorism Investigator's Handbook
Mafiaboy
Distributed Denial of Service Attacks
Webster's New World Hacker Dictionary
Computer Security Handbook, Set
Firewalls For Dummies
Real-world Detection and Mitigation
A Portrait of the Hacker as a Young Man
Profiling Hackers
Cyberthreats
Cyber Power
Concepts, Methodologies, Tools and Applications
The Rise of Information Geopolitics in U.S. National Security
Concepts, Methodologies, Tools, and Applications
Cyber Threat: The Rise of Information Geopolitics in U.S. National Security
1980 to Present
Mafiaboy
Cybercrime: An Encyclopedia of Digital Crime

BRAIDEN SANAA

Countering Terrorism Lulu.com
An examination of the social impact of the Internet, this volume explores political, social, technical, legal, and economic controversies in a manner accessible to the general reader. * A glossary of key terms, such as algorithm, ARPAnet, Hyper Text Markup Language, identity theft, Internet protocol, malicious mode, and Moore's law, helps readers find their bearings in the high-tech world of the Internet * Bibliographical sketches of 20 key personalities—both positive and negative—in Internet history bring this high-tech story to life
Confessions of Teenage Hackers Wilfrid Laurier Univ. Press
MafiaboyHow I Cracked the Internet and why It's Still BrokenPenguin Group Canada
UNB Law Journal MafiaboyHow I Cracked the Internet and why It's Still Broken
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

Cybersecurity Breaches and Issues Surrounding Online Threat Protection John Wiley & Sons

Distributed Denial of Service (DDoS) attacks have become more destructive, wide-spread and harder to control over time. This book allows students to understand how these attacks are constructed, the security flaws they leverage, why they are effective, how they can be detected, and how they can be mitigated. Students use software defined networking (SDN) technology to created and execute controlled DDoS experiments. They learn how to deploy networks, analyze network performance, and create resilient systems. This book is used for graduate level computer engineering instruction at Clemson University. It augments the traditional graduate computing curricula by integrating: Internet deployment, network security, ethics, contemporary social issues, and engineering principles into a laboratory based course of instruction. Unique features of this book include: A history of DDoS attacks that includes attacker motivations Discussion of cyber-war, censorship, and Internet black-outs SDN based DDoS laboratory assignments Up-to-date review of current DDoS attack techniques and tools Review of the current laws that globally relate to DDoS Abuse of DNS, NTP, BGP and other parts of the global Internet infrastructure to attack networks Mathematics of Internet traffic measurement Game theory for DDoS resilience Construction of content distribution systems that absorb DDoS attacks This book assumes familiarity with computing, Internet design, appropriate background in mathematics, and some programming skills. It provides analysis and reference material for networking engineers and researchers. By increasing student knowledge in security, and networking; it adds breadth and depth to advanced computing curricula.

Management Information Systems IGI Global

In 2000, an unknown attacker brought down the websites of Amazon, CNN, Dell, E-TRADE, eBay, and Yahoo!, inciting panic from Silicon Valley to the White House. The FBI, police, and independent security experts launched a manhunt as President Clinton convened a cyber security summit to discuss how best to protect America's information infrastructure from future attacks. Then, after hundreds of hours of wiretapping, law enforcement officials executed a late-night raid and came face-to-face with the most wanted man in cyberspace: a fifteen-year-old whose username was “Mafiaboy.” Despite requests from every major media outlet, that young man, Michael Calce, has never spoken publicly about his crimes—until now. Equal parts true-crime thriller and exposé, Mafiaboy will take you on an electrifying tour of the fast-evolving twenty-first-century world of hacking—from disruptions caused by teens like Calce to organized crime and other efforts with potentially catastrophic results. It also includes a guide to protecting yourself online.

Cybercrime and the Law Oxford University Press

Looks at how banks and their lending policies facilitate fraud and identity theft, revealing the many ways large lending institutions have put customers at risk to maximize profits.

Cyber Crimes IGI Global

Technology has become deeply integrated into modern society and various activities throughout everyday life. However, this increases the risk of vulnerabilities, such as hacking or system errors, among other online threats. Cybersecurity Breaches and Issues Surrounding Online Threat Protection is an essential reference source for the latest scholarly research on the various types of unauthorized access or damage to electronic data. Featuring extensive coverage across a range of relevant perspectives and topics, such as robotics, cloud computing, and electronic data diffusion, this publication is ideally designed for academicians, researchers, computer engineers, graduate students, and practitioners seeking current research on the threats that exist in the world of technology.

When Technocultures Collide Union Square Press

Written by experts for the general audience, this A-Z presentation covers all aspects of forensic science from its beginning to its central place in modern law enforcement.

Crime, Conflict and Security in Cyberspace John Wiley & Sons

Defines over eight hundred terms, including legal cases and people, related to computer hacking and computer security; provides a chronology of events related to hacking; and describes the ways in which hackers work.

Managing Information Technology in the Business Enterprise Syngress

Discusses the lives, careers, and motivations of computer hackers, profiling individuals and groups including Genocide, Mafiaboy, World of Hell, and Starla Pureheart.

A History of Cyber Security Attacks UPNE

Stories of cyberattacks dominate the headlines. Whether it is theft of massive amounts of personally identifiable information or the latest intrusion of foreign governments in U.S. government and industrial sites, cyberattacks are now important. For professionals and the public, knowing how the attacks are launched and succeed is vital to ensuring cyber security. The book provides a concise summary in a historical context of the major global cyber security attacks since 1980. Each attack covered contains an overview of the incident in layman terms, followed by a technical details section, and culminating in a lessons learned and recommendations section.

America's Battle Against Russia, China, and the Rising Global Cyber Threat MIT Press

Most books on cybercrime are written by national security or political experts, and rarely propose an integrated and comprehensive approach to cybercrime, cyber-terrorism, cyber-war and cyber-security. This work develops approaches to crucial cyber-security issues that are non-political, non-partisan, and non-governmental. It informs readers throug

A Reference Handbook Oxford University Press

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.

Computers and Society ABC-CLIO

Computer crime refers to criminal activity involving a computer. The computer may be used in the commission of a crime or it may be the target. This book covers the history of Cyber Crimes and gives some of the world's most famous Cyber Crime and Attacks.

Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and

Applications IGI Global
Complex and controversial, hackers possess a wily, fascinating talent, the machinations of which are shrouded in secrecy. Providing in-depth exploration into this largely uncharted territory, Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking offers insight into the hacking realm by telling attention-grabbing ta
Dawn of the Code War Jones & Bartlett Publishers
What an amazing world we live in! Almost anything you can imaginecan be researched, compared, admired, studied, and in many cases,bought, with the click of a mouse. The Internet has changed ourlives, putting a world of opportunity before us. Unfortunately, ithas also put a world of opportunity into the hands of those whosemotives are less than honorable. A firewall, a piece of software orhardware that erects a barrier between your computer and those whomight like to invade it, is one solution. If you've been using the Internet for any length of time,you've probably received some unsavory and unsolicitede-mail. If you run a business, you may be worried about thesecurity of your data and your customers' privacy. At home,you want to protect your personal information from identity thievesand other shady characters. Firewalls ForDummies® will give you the lowdown onfirewalls, then guide you through choosing, installing, andconfiguring one for your personal or bus iness network. Firewalls For Dummies® helps youunderstand what firewalls are, how they operate on different typesof networks, what they can and can't do, and how to pick agood one (it's easier than identifying that perfect melon inthe supermarket.) You'll find out about Developing security policies Establishing rules for simple protocols Detecting and responding to system intrusions Setting up firewalls for SOHO or personal use Creating demilitarized zones Using Windows or Linux as a firewall Configuring ZoneAlarm, BlackICE, and Norton personalfirewalls Installing and using ISA server and FireWall-1 With the handy tips and hints this book provides, you'llfind that firewalls are nothing to fear – that is,unless you're a cyber-crook! You'll soon be able tokeep your data safer, protect your family's privacy, andprobably sleep better, too.
The Emerging Fault Lines of the Nation State CRC Press
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
Computer Investigation Pearson P T R
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.
Cyber Crime: Concepts, Methodologies, Tools and Applications Rowman & Littlefield
Michel Calce, connu mondialement sous le nom de Mafiaboy, raconte, avec l'aide du journaliste Craig Silverman, comment il est devenu à l'âge de quinze ans un des pirates informatiques les plus recherchés, son arrestation par la GRC et son histoire personnelle. [SDM].
Greed, Corruption, Villains, and Victims IGI Global
In early 2000, the websites of CNN, Yahoo, E*Trade, Dell, Amazon, and eBay ground to a halt for several hours, causing panic everywhere from the White House to suburbia and around the world. After 2 months and hundreds of hours of wiretapping, the FBI and RCMP staged a late-night raid to apprehend the most wanted man in cyberspace--a 15-year-old kid, Mafiaboy. 8 years later, Mafiaboy, a.k.a.Michael Calce, has ignored requests from every major media outlet in North America and has not told a word of his story--until now. Using his experience as a cautionary tale, Calce takes the reader through the history of hacking and how it has helped make the internet the new frontier for crime in the 21st century.