Mafiaboy

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.

For more than 20 years, Network World has been the premier provider of information, intelligence and insight for network and IT executives responsible for the digital nervous systems of large organizations. Readers are responsible for designing, implementing and managing the voice, data and video systems their companies use to support everything from business critical applications to employee collaboration and electronic commerce.

Traces the story of how a computer hacker crashed several of the world's biggest websites, causing $1.2 billion in damage and inciting panic, in an account that exposes the insidious nature of rapidly evolving Internet crime.

For more than 40 years, Computerworld has been the leading source of technology news and information for IT influencers worldwide. Computerworld's award-winning Web site (Computerworld.com), twice-monthly publication, focused conference series and custom research form the hub of the world's largest global IT media network.

Lucia It all started with a contract signed by him, then by me, while our families watched. While my father sat silent, a man defeated, giving his daughter to the Benedetti monsters. I obeyed. I played my part. I signed my name and gave away my life. I became their living, breathing trophy, a constant symbol of their power over us. That was five years ago. Then came the time for him to claim me. For Salvatore Benedetti to own me. I had vowed vengeance. I had learned hate. And yet, nothing could have prepared me for the man who now ruled my life. I expected a monster, one I would destroy. But nothing is ever black or white. No one is either good or evil. For all his darkness, I saw his light. For all his evil, I saw his good. As much as he made me hate him, a passion hotter than the fires of hell burned inside me. I was his, and he was mine. My very own monster. Salvatore I owned the DeMarco Mafia Princess. She belonged to me now. We had won, and they had lost. And what better way to teach a lesson than to take from them that which is most precious? Most beloved? I was the boy who would be king. Next in line to rule the Benedetti Family. Lucia DeMarco was the spoils of war. Mine to do with as I pleased. It was my duty to break her. To make her life a living hell. My soul was dark, I was hell bound. And there was no way out, not for either of us. Because the Benedetti family never lost, and in our wake, we left destruction. It’s how it had always been. How I believed it would always be. Until Lucia.

MafiaboyA Portrait of the Hacker as a Young ManRowman & 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].

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.

Ways in which federal, state, and local institutions should integrate their efforts to prepare for future terrorist threats.

As new technologies develop, terrorist groups are developing new methods of attack by using the Internet, and by using cyberspace as a battlefield, it has become increasingly difficult to discover the identity of attackers and bring them to justice. The seemingly limitless boundaries of cyberspace has allowed virtually anyone to launch an attack from a remote and anonymous location. But once these attacks occur, it raises several important questions; who should respond, and how?; how should nation-states effectively deal with a cyber-attack?; and will the United States and other nation-states be able to survive in a world where virtual boundaries are limitless? In Cyberthreats: The Emerging Fault Lines of the Nation State Susan Brenner gives a thorough explanation of how military and law enforcement personnel respond to these attacks and why bringing cyber-terrorist to justice can be difficult and sometimes impossible.

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.

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

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.

Computer security touches every part of our daily lives from our computers and connected devices to the wireless signals around us. Breaches have real and immediate financial, privacy, and safety consequences. This handbook has compiled advice from top professionals

working in the real world about how to minimize the possibility of computer security breaches in your systems. Written for professionals and college students, it provides comprehensive best guidance about how to minimize hacking, fraud, human error, the effects of natural disasters, and more. This essential and highly-regarded reference maintains timeless lessons and is fully revised and updated with current information on security issues for social networks, cloud computing, virtualization, and more.

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.

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.

Jonathan Lusthaus lifts the veil on cybercriminals in the most extensive account yet of the lives they lead and the vast international industry they have created. Having traveled to hotspots around the world to meet with hundreds of law enforcement agents, security gurus, hackers, and criminals, he charts how this industry based on anonymity works.

To many who knew him, there was nothing odd about him. He was a normal kid ... On February 7, 2000, Yahoo.com was the first victim of the biggest distributed denial-of-service attack ever to hit the Internet. On May 8th, Buy.com was battling a massive denial-of-service attack. Later that afternoon, eBay.com also reported significant outages of service, as did Amazon.com. Then CNN's global online news operation started to grind to a crawl. By the following day, Datek and E-Trade entered crisis mode ... all thanks to an ordinary fourteen-year-old kid. Friends and neighbors were shocked to learn that the skinny, dark-haired, boy next door who loved playing basketball--almost as much as he loved computers--would cause millions of dollars worth of damage on the Internet and capture the attention of the online world--and the federal government. He was known online as "Mafiaboy" and, to the FBI, as the most notorious teenage hacker of all time. He did it all from his bedroom PC. And he's not alone.

Presents an overview of the history of computer crime as well as case studies to show the affect various events had on shaping the views of computer crime in the United States.

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

When Technocultures Collide provides rich and diverse studies of collision courses between technologically inspired subcultures and the corporate and governmental entities they seek to undermine. The adventures and exploits of computer hackers, phone phreaks, urban explorers, calculator and computer collectors, “CrackBerry” users, whistle-blowers, Yippies, zinsters, roulette cheats, chess geeks, and a range of losers and tinkerers feature prominently in this volume. Gary Genosko analyzes these practices for their remarkable diversity and their innovation and leaps of imagination. He assesses the results of a number of operations, including the Canadian stories of Mafiaboy, Jeff Chapman of Infiltration, and BlackBerry users. The author provides critical accounts of highly specialized attributes, such as the prospects of deterritorialized computer mice and big toe computing, the role of electrical grid hacks in urban technopolitics, and whether info-addiction and depression contribute to tactical resistance. Beyond resistance, however, the goal of this work is to find examples of technocultural autonomy in the minor and marginal cultural productions of small cultures, ethico-poetic diversions, and sustainable withdrawals with genuine therapeutic potential to surpass accumulation, debt, and competition. The dangers and joys of these struggles for autonomy are underlined in studies of RIM’s BlackBerry and Julian Assange’s WikiLeaks website.

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.

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.

"This book explores the ethical challenges of technology innovations, providing cutting-edge analysis of designs, developments, impacts, policies, theories, and methodologies related to ethical aspects of technology in society"--Provided by publisher.

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.

The digital age we entered in the twenty-first century has rapidly become an age of digital crime. Cybercrimes like spoofing, phishing, and hacking are on the rise, and computer forensic technicians are on the case. Even "traditional" crimes like murder, fraud, and child abuse can be both facilitated by computers—and solved through computer investigation. Computer Investigation helps readers understand how cybercrimes are committed, and how investigators help solve them and bring the perpetrators to justice. Readers will also gain a few tips for protecting themselves online and protecting their computers from intrusions and hacks.

"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.

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 first full-scale overview of cybercrime, law, and policy

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.

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

A stunning debut novel with an intriguing literary hook: written in part as a letter from a victim to her abductor. Sensitive, sharp, captivating! Gemma, 16, is on layover at Bangkok Airport, en route with her parents to a vacation in Vietnam. She steps away for just a second, to get a cup of coffee. Ty--rugged, tan, too old, oddly familiar--pays for Gemma's drink. And drugs it. They talk. Their hands touch. And before Gemma knows what's happening, Ty takes her. Steals her away. The unknowing object of a long obsession, Gemma has been kidnapped by her stalker and brought to the desolate Australian Outback. STOLEN is her gripping story of survival, of how she has to come to terms with her living nightmare--or die trying to fight it.

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

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

Winner of the National Press Club's Arthur Rowse Award for Press Criticism! From Craig Silverman, proprietor of www.RegretTheError.com, comes a lively journey through the history of media mistakes via a chronicle of funny, shocking, and often disturbing journalistic slip-ups. The errors—running the gamut from hilarious to tragic—include “Fuzzy Numbers” (when numbers and math undermine reporting) “Obiticide” (printing the obituary of a living person), and “Unintended Consequences” (typos and misidentifications that create a new, incorrect reality). While some of the errors are laugh-out-loud funny, the book also offers a serious investigation of contemporary journalism's lack of accountability to the public, and a rousing call to arms for all news organizations to mend their ways and reclaim the role of the press as honest voice of the people.

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

Documents how a troubled young computer hacker seized control of a massive international computer fraud network in 2006, tracing the efforts of FBI and Secret Service agents as well as an undercover operator to locate and arrest him. Reprint.

The Internet is often called a superhighway, but it may be more analogous to a city: an immense tangle of streets, highways, and interchanges, lined with homes and businesses, playgrounds and theatres. We may not physically live in this city, but most of us spend a lot of time there, and even pay rents and fees to hold property in it. But the Internet is not a city of the 21st century. Jeffrey Hunker, an internationally known expert in cyber-security and counter-terrorism policy, argues that the Internet of today is, in many ways, equivalent to the burgeoning cities of the early Industrial Revolution: teeming with energy but also with new and previously unimagined dangers, and lacking the technical and political infrastructures to deal with these problems. In a world where change of our own making has led to unexpected consequences, why have we failed, at our own peril, to address these consequences? Drawing on his experience as a top expert in information security, Hunker sets out to answer this critical question in Creeping

Failure. Hunker takes a close look at the "creeping failures" that have kept us in a state of cyber insecurity: how and why they happened, and most crucially, how they can be fixed. And he arrives at some stunning conclusions about the dramatic measures that we will need to accomplish this. This groundbreaking book is an essential first step toward understanding the World Wide Web in a larger context as we try to build a safer Internet "city." But it also raises issues that are relevant far outside the online realm: for example, how can we work together to create not just new policy, but new kinds of policy? Creeping Failure calls for nothing less than a basic rethinking of the Internet — and of how we solve problems together.

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.