Hacked Credit Cards Details Bing

Off the Back of a Truck
Facebook Nation
When Did I Start Looking Like a Cop?
The Metaweb
The Darkening Web
Cybercrime
Returning to Interpersonal Dialogue and Understanding Human Communication in the Digital Age
The World Almanac and Book of Facts 2023
My Paperback Book
Biomedical Defense Principles to Counter DNA Deep Hacking
DK Eyewitness Travel Guide USA
Cybersafe for Business
Hacking Web Intelligence
Drugs & Society
Fighting Phishing
Kingpin
Handbook on Crime and Technology
Advancements in Cybercrime Investigation and Digital Forensics
Research Anthology on Child and Domestic Abuse and Its Prevention
Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions
Combating the Exploitation of Children in Cyberspace: Emerging Research and Opportunities
Dark World
Perfect Vision
The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age
Decoding Generative AI
The World Almanac and Book of Facts 2022
Selling Rights
Certified Ethical Hacker (CEH) v12 312-50 Exam Guide
الشندغة
19th International Conference on Cyber Warfare and Security
Web Data Mining with Python
Advances in Biometric Person Authentication
Rethinking Organised Crime
Low Tech Hacking
Dissecting the Hack: The F0rb1dd3n Network, Revised Edition
Cybercrime and Digital Forensics
Cyber Security Essentials
Digital Criminology
Emerging Threats and Countermeasures in Cybersecurity
Social Media Security

MILLER PRECIOUS

Off the Back of a Truck
Routledge
This book explores total information awareness empowered by social media. At the FBI Citizens Academy in February 2021, I asked the FBI about the January 6 Capitol riot organized on social media that led to the unprecedented ban of a sitting U.S. President by all major social networks. In March 2021, Facebook CEO Mark Zuckerberg, Google CEO Sundar Pichai, and Twitter CEO Jack Dorsey appeared before Congress to face criticism about their handling of misinformation and online extremism that culminated in the storming of Capitol Hill. With more than three billion monthly active users, Facebook family of apps is by far the world's largest social network. Facebook as a nation is bigger than the top three most populous countries in the world: China, India, and the United States. Social media has enabled its users to inform and misinform the public, to appease and disrupt Wall Street, to mitigate and exacerbate the COVID-19 pandemic, and to unite and divide a country. Mark Zuckerberg once said, "We exist at the intersection of technology and social issues." He should have heeded his own words. In October 2021, former Facebook manager-turned-whistleblower Frances Haugen testified at the U.S. Senate that Facebook's products "harm children, stoke division, and weaken our democracy." This book offers discourse and practical advice on information and misinformation, cybersecurity and privacy issues, cryptocurrency and business intelligence, social media marketing and caveats, e-government and e-activism, as well as the pros and cons of total information awareness including the Edward Snowden leaks. "Highly recommended." - T. D. Richardson, Choice Magazine "A great book for social media experts." - Will M., AdWeek "Parents in particular would be well advised to make this book compulsory reading for their teenage children..." - David B. Henderson, ACM Computing Reviews
Facebook Nation Springer Nature
Unleash your inner Soprano and relive all your favorite moments with this companion guide to the award-winning television series The Sopranos. We all know and love The Sopranos, one of the most important television dramas to ever hit the small screen, having run for six seasons on HBO. The story of the Italian-American mobster Tony Soprano balancing his family life with his role as the leader of a criminal organization pioneered decades of genre-bending “peak TV.” Now, Off the Back of a Truck takes you one step further into the world of Tony Soprano and his families, offering an Italian potluck of fresh and fun takes that any true fan can get lost in for hours. Off the Back of a Truck includes: -New looks at everyone’s favorite episodes, scenes, and characters -All 92 deaths analyzed, evaluated, and ranked -An investigation of true crimes behind the families’ schemes -An exploration of movies and shows that inspired The Sopranos -Reflections on the use of music, food, and fashion from writers who are also huge fans -A provocative conversation about what happens in the controversial ending This book takes you on a

journey through the six seasons you have watched time and time again—but it's organized so you can dip in at any time, at any place. Roam around as though you're in Tony's backyard for a BBQ...

When Did I Start Looking Like a Cop? Lulu.com

Explore different web mining techniques to discover patterns, structures, and information from the web KEY FEATURES ● A complete overview of the basic and advanced concepts of Web mining. ● Work with easy-to-use open-source Python libraries for Web mining. ● Get familiar with the various beneficial areas and applications of Web mining. DESCRIPTION Data Science is the fastest growing job across the globe and is predicted to create 11.5 million jobs by 2026, so job seekers with this skill set have a lot of opportunities. One of the most sought areas in the field of Data Science is mining information from the web. If you are an aspiring Data Scientist looking to learn different Web mining techniques, then this book is for you. This book starts by covering the key concepts of Web mining and its taxonomy. It then explores the basics of Web scraping, its uses and components followed by topics like legal aspects related to scraping, data extraction and pre-processing, scraping dynamic websites, and CAPTCHA. The book also introduces you to the concept of Opinion mining and Web structure mining. Furthermore, it covers Web graph mining, Web information extraction, Web search and hyperlinks, Hyperlink Induced Topic Search (HITS) search, and partitioning algorithms that are used for Web mining. Towards the end, the book will teach you different mining techniques to discover interesting usage patterns from Web data. By the end of the book, you will master the art of data extraction using Python. WHAT YOU WILL LEARN ● Learn how to scrape data from any website with Python. ● Get familiar with the concepts of Opinion Mining and Sentiment Analysis. ● Use Web structure mining to discover structure information from the web. ● Learn how to collect and analyze social media data using Python. ● Use Web usage mining for predicting users' browsing behaviors. WHO THIS BOOK IS FOR The book is for anyone who wants to learn Web mining. Aspiring Data Scientists, Data Engineers, and Data Analysts who want to master Web mining will find this book very helpful. TABLE OF CONTENTS 1. Web Mining—An Introduction 2. Web Mining Taxonomy 3. Prominent Applications with Web Mining 4. Python Fundamentals 5. Web Scraping 6. Web Opinion Mining 7. Web Structure Mining 8. Social Network Analysis in Python 9. Web Usage Mining

The Metaweb Dorling Kindersley Ltd

This book is an essential resource for anyone seeking to stay ahead in the dynamic field of cybersecurity, providing a comprehensive toolkit for understanding and combating digital threats and offering practical, insightful guidance ideal for cybersecurity professionals, digital forensic investigators, legal practitioners, law enforcement, scholars, and students. In the rapidly evolving domain of digital security, this book emerges as a vital guide for understanding and addressing the sophisticated landscape

of cyber threats. This in-depth volume, featuring contributions from renowned experts, provides a thorough examination of the current state and future challenges in digital security and forensic analysis. The book is meticulously organized into seven sections (excluding conclusion), each focusing on a critical aspect of cybersecurity. It begins with a comprehensive overview of the latest trends and threats in the field, setting the stage for deeper explorations in subsequent sections. Readers will gain insights into a range of topics, from the intricacies of advanced persistent threats and malware, to the security nuances of cyber-physical systems and the Internet of Things (IoT). The book covers cutting-edge topics like blockchain, cryptography, social engineering, cloud security, and data privacy, blending theory with practical case studies. It’s a practical guide for cybersecurity professionals, forensic investigators, legal practitioners, law enforcement, scholars, and students. Offering a comprehensive toolkit for combating digital threats, it’s essential for staying ahead in the fast-evolving field of cybersecurity.

The Darkening Web W. W. Norton & Company

A Brooklyn native, Joseph Belcastro joined the New York City Police Department in July, 1983. He spent four years on uniform patrol, then another four years in the precincts plainclothes Anti-Crime Unit, before being transferred to the NYPDs infamous Street Crime Unit on Randalls Island. In his tell-all memoir, Joe describes his earliest encounters as a rookie cop in uniform, how he developed his unique crime-fighting strategies, and the partners he had along the way. Joes uncanny ability to follow his gut instincts, along with his determination and perseverance, led him to personally make over a thousand arrests, and to assist his partners in at least a thousand more. Ride along with Joe on his vehicle pursuits, sit in the back seat of his car stops, and in the process share the triumphs and disappointments in the life of a street cop. Its a ride you wont want to miss!

Cybercrime Academic Conferences and publishing limited

Keep valuable data safe from even the most sophisticated social engineering and phishing attacks Fighting Phishing: Everything You Can Do To Fight Social Engineering and Phishing serves as the ideal defense against phishing for any reader, from large organizations to individuals. Unlike most anti-phishing books, which focus only on one or two strategies, this book discusses all the policies, education, and technical strategies that are essential to a complete phishing defense. This book gives clear instructions for deploying a great defense-in-depth strategy to defeat hackers and malware. Written by the lead data-driven defense evangelist at the world's number one anti-phishing company, KnowBe4, Inc., this guide shows you how to create an enduring, integrated cybersecurity culture. Learn what social engineering and phishing are, why they are so dangerous to your cybersecurity, and how to defend against them Educate yourself and other users on how to identify and avoid phishing scams, to stop attacks before they begin Discover the latest tools and strategies for locking down data when phishing

has taken place, and stop breaches from spreading Develop technology and security policies that protect your organization against the most common types of social engineering and phishing Anyone looking to defend themselves or their organization from phishing will appreciate the uncommonly comprehensive approach in Fighting Phishing.

Returning to Interpersonal Dialogue and Understanding Human Communication in the Digital Age CRC Press Discover the hidden depths of the digital underworld in this comprehensive, interdisciplinary exploration of the dark web. Ideal for security agencies, professionals, counter-terrorism experts, and policymakers alike, this work offers invaluable insights that will enhance understanding and fortify strategies. By shedding particular light on the nuances of the ‘dark market,’ this book provides readers with a detailed understanding of the dark web, encompassing both its sinister underbelly and unexpected potential. This book also uncovers the latest trends and cutting-edge mitigation techniques. From illicit transactions to thriving business ventures, it examines the key domains and sectors that thrive within this clandestine environment. This book consolidates myriad perspectives on security and threats on the dark web.

The World Almanac and Book of Facts 2023 Edward Elgar Publishing Biomedical Defense Principles to Counter DNA Deep Hacking presents readers with a comprehensive look at the emerging threat of DNA hacking. Dr. Rocky Termanini goes in-depth to uncover the erupting technology being developed by a new generation of savvy bio-hackers who have skills and expertise in biomedical engineering and bioinformatics. The book covers the use of tools such as CRISPR for malicious purposes, which has led agencies such as the U.S. Office of the Director of National Intelligence to add gene editing to its annual list of threats posed by "weapons of mass destruction and proliferation." Readers will learn about the methods and possible effects of bio-hacking attacks, and, in turn the best methods of autonomic and cognitive defense strategies to detect, capture, analyze, and neutralize DNA bio-hacking attacks, including the versatile DNA symmetrical AI Cognitive Defense System (ACDS). DNA bio-hackers plan to destroy, distort and contaminate confidential, healthy DNA records and potentially create corrupted genes for erroneous diagnosis of illnesses, disease genesis and even wrong DNA fingerprinting for criminal forensics investigations. - Presents a comprehensive reference for the fascinating emerging technology of DNA storage, the first book to present this level of detail and scope of coverage of this groundbreaking field - Helps readers understand key concepts of how DNA works as an information storage system and how it can be applied as a new technology for data storage - Provides readers with key technical understanding of technologies used to work with DNA data encoding, such as CRISPR, as well as emerging areas of application and ethical concern, such as smart cities, cybercrime, and cyber warfare - Includes coverage of synthesizing

DNA-encoded data, sequencing DNA-encoded data, and fusing DNA with Digital Immunity Ecosystem (DIE)

My Paperback Book IntelX Publishing

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.

Biomedical Defense Principles to Counter DNA Deep Hacking iUniverse

Markets are good because they facilitate economic efficiency, but when that efficiency facilitates criminal activity; such "black markets" can be deemed harmful. Business and Global business require a stable environment in which to operate. The more chaos, the more difficult is to successfully do business. However as businesses expand around the world, many will take more risks and begin operating in foreign nation-states that may not have stable government and indeed may be the home of one or more groups of miscreants.Financial Institutions and other business enterprises are required to take strong measures to protect their assets as they are operating in global information technology. This essay review how 100 Banks Got Hacked and Lost $900 Million and proposes twenty (20) Ways to Keep Safe from Hackers while doing online businesses.

DK Eyewitness Travel Guide USA Simon and Schuster

This book examines the concept and elements of the digital world; technologies of the digital world in the era of the third and fourth industrial revolutions; criminogenic factors present in the era of the third and fourth industrial revolutions; features of crime, terrorism, and extremism in the digital world; the identity of criminals and criminal organizations operating in the digital

world; and measures to prevent crime in the digital world.

Cybersafe for Business
BPB Publications
5 Stars! from Doody's Book Reviews! (of the 13th Edition) "This edition continues to raise the bar for books on drug use and abuse. The presentation of the material is straightforward and comprehensive, but not off putting or complicated." As a long-standing, reliable resource Drugs & Society, Fourteenth Edition continues to captivate and inform students by taking a multidisciplinary approach to the impact of drug use and abuse on the lives of average individuals. The authors have integrated their expertise in the fields of drug abuse, pharmacology, and sociology with their extensive experiences in research, treatment, drug policy making, and drug policy implementation to create an edition that speaks directly to students on the medical, emotional, and social damage drug use can cause.

Hacking Web Intelligence
CRC Press
The sophisticated methods used in recent high-profile cyber incidents have driven many to need to understand how such security issues work. Demystifying the complexity often associated with information assurance, Cyber Security Essentials provides a clear understanding of the concepts behind prevalent threats, tactics, and procedures.To accomplish

Drugs & Society
Routledge
Former hacker Kevin Poulsen has, over the past decade, built a reputation as one of the top investigative reporters on the cybercrime beat. In Kingpin, he pours his unmatched access and expertise into book form for the first time, delivering a gripping cat-and-mouse narrative—and an unprecedented view into the twenty-first century’s signature form of organized crime. The word spread through the hacking underground like some unstoppable new virus: Someone—some brilliant, audacious crook—had just staged a hostile takeover of an online criminal network that siphoned billions of dollars from the US economy. The FBI rushed to launch an ambitious undercover operation aimed at tracking down this new kingpin; other agencies around the world deployed dozens of moles and double agents. Together, the cybercops lured numerous unsuspecting hackers into their clutches. . . . Yet at every turn, their main quarry displayed an uncanny ability to sniff out their snitches and see through their plots. The culprit they sought was the most unlikely of criminals: a brilliant programmer with a hippie ethic and a supervillain’s double identity. As prominent “white-hat” hacker Max “Vision” Butler, he was a celebrity throughout the programming world, even serving as a consultant to the FBI. But as the black-hat “Iceman,” he found in the world of data theft an irresistible opportunity to test his outsized abilities. He infiltrated thousands of computers around the country, sucking down millions of credit card numbers at will. He effortlessly hacked his fellow hackers, stealing their ill-gotten gains from under their noses. Together with a smooth-talking con artist, he ran a massive real-world crime ring. And for years, he did it all with seeming impunity, even as countless rivals ran afoul

of police. Yet as he watched the fraudsters around him squabble, their ranks riddled with infiltrators, their methods inefficient, he began to see in their dysfunction the ultimate challenge: He would stage his coup and fix what was broken, run things as they should be run—even if it meant painting a bull's-eye on his forehead. Through the story of this criminal's remarkable rise, and of law enforcement's quest to track him down, Kingpin lays bare the workings of a silent crime wave still affecting millions of Americans. In these pages, we are ushered into vast online-fraud supermarkets stocked with credit card numbers, counterfeit checks, hacked bank accounts, dead drops, and fake passports. We learn the workings of the numerous hacks—browser exploits, phishing attacks, Trojan horses, and much more—these fraudsters use to ply their trade, and trace the complex routes by which they turn stolen data into millions of dollars. And thanks to Poulsen's remarkable access to both cops and criminals, we step inside the quiet, desperate arms race that law enforcement continues to fight with these scammers today. Ultimately, Kingpin is a journey into an underworld of startling scope and power, one in which ordinary American teenagers work hand in hand with murderous Russian mobsters and where a simple Wi-Fi connection can unleash a torrent of gold worth millions.

Fighting Phishing Bloomsbury Publishing USA

Every day, both adults and children are victimized in unhealthy relationships. Domestic and child abuse have surged during the COVID-19 pandemic as potential escapes from abuse at home were stripped away. Abuse is a raging global issue; however, with enough research, policy, and social activism, society can aid in the prevention of child and domestic abuse. The Research Anthology on Child and Domestic Abuse and Its Prevention discusses the prevalence of domestic abuse as well as the exploitation of children both at home and beyond. It further presents emerging practices in technology, social work, and criminology to prevent the further exploitation and victimization of adults and children in abusive situations. Covering topics such as foster children, gender-based violence, and trauma analysis, this major reference work is an indispensable resource for social workers, lawmakers, government organizations, non-profit organizations, psychologists, therapists, sociologists, libraries, students and educators of higher education, criminologists, leaders in law enforcement, researchers, and academicians.

Kingpin Crown

Selling Rights has firmly established itself as the leading guide to all aspects of rights sales and co-publications throughout the world. The seventh edition is substantially updated to illustrate the changes in rights in relation to new technologies and legal developments in the United Kingdom and the rest of the world. This fully revised and updated edition includes: coverage of the full range of potential rights from English-language territorial rights through to serial rights, permissions, rights for the reading-impaired, translation rights, dramatization and

documentary rights, electronic and multimedia rights More detailed coverage of Creative Commons and Open Access The aftermath of the Digital Economy Act 2010, the Hooper Report and new UK Statutory Instruments affecting copyright Updated coverage of book fairs The implications of adding e-book rights to print licences A separate chapter on collective licensing via Reproduction Rights Organizations The impact of new electronic hardware (e-readers, tablets, mobile phones) – the distinction between sales and licences the rights implications of acquisitions, mergers and disposals updates on serial rights, including online New appendices listing territories normally sought as exclusive by UK publishers and a glossary of rights specific terms. Selling Rights is an essential reference tool and an accessible and illuminating guide to current and future issues for rights professionals and students of publishing.

Handbook on Crime and Technology

Springer

Buckle up for a fascinating journey through layers of insight and metaphors that explain the past, present, and future of the Web. Readers from all walks of life will learn something ancient, something novel, and something practical. Those who give it careful consideration will never see the Web the same way again. This book proclaims into existence decentralized public space above the webpage that enables the shift from personal to collective computing. The Web's next frontier is the Metaweb, a hyper-dimensional web over Today's Web that connects people and information silos, with accountability and fair value exchange. The Metaweb can drastically reduce false information, abuse, and scams, as well as enable the unprecedented level of collaboration needed to address humanity's global challenges. The book posits a symbiotic relationship between AI and the Metaweb, where AI assists in generating, organizing, and curating content, while the Metaweb provides the necessary constraints, data, and context for AI to function effectively, transparently, and in alignment with humanity. The AI-assisted collaboration among humans on the Metaweb will enable a vast collective intelligence and the capture of tremendous untapped value. For more information go to: http://metawebbook.com

Advancements in Cybercrime Investigation and Digital Forensics

Packt Publishing Ltd

Learn to defend crucial ICS/SCADA infrastructure from devastating attacks the tried-and-true Hacking Exposed way This practical guide reveals the powerful weapons and devious methods cyber-terrorists use to compromise the devices, applications, and systems vital to oil and gas pipelines, electrical grids, and nuclear refineries. Written in the battle-tested Hacking Exposed style, the book arms you with the skills and tools necessary to defend against attacks that are debilitating—and potentially deadly. Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions explains vulnerabilities and attack vectors specific to ICS/SCADA protocols, applications, hardware, servers, and workstations. You will learn how hackers

and malware, such as the infamous Stuxnet worm, can exploit them and disrupt critical processes, compromise safety, and bring production to a halt. The authors fully explain defense strategies and offer ready-to-deploy countermeasures. Each chapter features a real-world case study as well as notes, tips, and cautions. Features examples, code samples, and screenshots of ICS/SCADA-specific attacks Offers step-by-step vulnerability assessment and penetration test instruction Written by a team of ICS/SCADA security experts and edited by Hacking Exposed veteran Joel Scambray

Research Anthology on Child and Domestic Abuse and Its Prevention Dragonsoul Books

A complex phenomenon which has undergone significant changes in the past forty years, Leslie Holmes argues that organised crime is in need of re-conceptualisation. This innovative book navigates the evolution of this issue to grasp its full scope in the twenty-first century.

Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions Penguin

This important reference work is an extensive, up-to-date resource for students who want to investigate 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.