Kingpin How One Hacker Took Over The Billion Dolla

If you ally obsession such a referred **kingpin how one hacker took over the billion dolla** book that will manage to pay for you worth, get the definitely best seller from us currently from several preferred authors. If you want to comical books, lots of novels, tale, jokes, and more fictions collections are afterward launched, from best seller to one of the most current released.

You may not be perplexed to enjoy every book collections kingpin how one hacker took over the billion dolla that we will extremely offer. It is not something like the costs. Its approximately what you infatuation currently. This kingpin how one hacker took over the billion dolla, as one of the most involved sellers here will unconditionally be accompanied by the best options to review.

Ghost in the Wires Kevin Mitnick 2011-08-15 In this "intriguing, insightful and extremely educational" novel, the world's most famous hacker teaches you easy cloaking and counter-measures for citizens and consumers in the age of Big Brother and Big Data (Frank W. Abagnale). Kevin Mitnick was the most elusive computer break-in artist in history. He accessed computers and networks at the world's biggest companies -- and no matter how fast the authorities were, Mitnick was faster, sprinting through phone switches, computer systems, and cellular networks. As the FBI's net finally began to tighten, Mitnick went on the run, engaging in an increasingly sophisticated game of hide-and-seek that escalated through false identities, a host of cities, and plenty of close shaves, to an ultimate showdown with the Feds, who would stop at nothing to bring him down. Ghost in the Wires is a thrilling true story of intrigue, suspense, and unbelievable escapes -- and a portrait of a visionary who forced the authorities to rethink the way they pursued him, and forced companies to rethink the way they protect their most sensitive information. "Mitnick manages to make breaking computer code sound as action-packed as robbing a bank." -- NPR

The Masters of Deception Michele Slatalla 1995-12-01 The bestselling account of a band of kids from New York who fought an electronic turf war that ranged across some of the nation's most powerful computer systems. "An immensely fun and -- one cannot emphasize this enough -- accessible history of the first outlaws in cyberspace."--Glamour

How to Steal a Million Sergey Pavlovich 2018-05-08 Sergey Pavlovich was a poor, talented boy from Belarus who made it big in the Russian-speaking hacking world of the early 2000s and earned millions of dollars from credit card fraud in just a few years. But he ended up in jail as a result of an FBI-led bust of what was dubbed the "largest and most complex identity theft in U.S. history."

He spent his twenties in Belarus' brutal prison system. This is the tell-all story of Pavlovich's meteoric rise in the hacking world and his spectacular fall. It is packed with details about the shadowy cyber-crime world and the lucrative credit card fraud schemes and spamming operations he and his friends devised. Learn about some of the colorful personalities from the first flowering of Slavic cyber-crime in Russia, Belarus and Ukraine and be horrified by Pavlovich's experience in prisons that have changed little since Soviet times. Most famously, Pavlovich was involved in a fraud ring run by notorious U.S. hacker Albert Gonzalez, who led a double life as an informer for American intelligence. The losses caused by Gonzalez and his friends were estimated to have exceeded $1 billion. This book, written by Pavlovich while in prison, has already been enjoyed by more than 50,000 Russian readers.

The Art of Deception Kevin D. Mitnick 2011-08-04 The world's most infamous hacker offers an insider's view of the low-tech threats to high-tech security Kevin Mitnick's exploits as a cyber-desperado and fugitive form one of the most exhaustive FBI manhunts in history and have spawned dozens of articles, books, films, and documentaries. Since his release from federal prison, in 1998, Mitnick has turned his life around and established himself as one of the most sought-after computer security experts worldwide. Now, in The Art of Deception, the world's most notorious hacker gives new meaning to the old adage, "It takes a thief to catch a thief." Focusing on the human factors involved with information security, Mitnick explains why all the firewalls and encryption protocols in the world will never be enough to stop a savvy grifter intent on rifling a corporate database or an irate employee determined to crash a system. With the help of many fascinating true stories of successful attacks on business and government, he illustrates just how susceptible even the most locked-down information systems are to a slick con artist impersonating an IRS agent. Narrating from the points of view of both the attacker and the victims, he explains why each attack was so successful and how it could have been prevented in an engaging and highly readable style reminiscent of a true-crime novel. And, perhaps most importantly, Mitnick offers advice for preventing these types of social engineering hacks through security protocols, training programs, and manuals that address the human element of security.

Hacking the Hacker Roger A. Grimes 2017-04-18 Meet the world's top ethical hackers and explore the tools of the trade Hacking the Hacker takes you inside the world of cybersecurity to show you what goes on behind the scenes, and introduces you to the men and women on the front lines of this technological arms race. Twenty-six of the world's top white hat hackers, security researchers, writers, and leaders, describe what they do and why, with each profile preceded by a no-experience-necessary explanation of the relevant technology. Dorothy Denning discusses advanced persistent threats, Martin Hellman describes how he helped invent public key encryption, Bill Cheswick talks about firewalls, Dr. Charlie Miller talks about hacking cars, and other cybersecurity experts from around the world detail the threats, their defenses, and the tools and techniques they use to thwart the most advanced criminals history has ever seen. Light on jargon and heavy on intrigue, this book is

designed to be an introduction to the field; final chapters include a guide for parents of young hackers, as well as the Code of Ethical Hacking to help you start your own journey to the top. Cybersecurity is becoming increasingly critical at all levels, from retail businesses all the way up to national security. This book drives to the heart of the field, introducing the people and practices that help keep our world secure. Go deep into the world of white hat hacking to grasp just how critical cybersecurity is Read the stories of some of the world's most renowned computer security experts Learn how hackers do what they do—no technical expertise necessary Delve into social engineering, cryptography, penetration testing, network attacks, and more As a field, cybersecurity is large and multi-faceted—yet not historically diverse. With a massive demand for qualified professional that is only going to grow, opportunities are endless. Hacking the Hacker shows you why you should give the field a closer look.

CUCKOO'S EGG Clifford Stoll 2012-05-23 Before the Internet became widely known as a global tool for terrorists, one perceptive U.S. citizen recognized its ominous potential. Armed with clear evidence of computer espionage, he began a highly personal quest to expose a hidden network of spies that threatened national security. But would the authorities back him up? Cliff Stoll's dramatic firsthand account is "a computer-age detective story, instantly fascinating [and] astonishingly gripping" (Smithsonian). Cliff Stoll was an astronomer turned systems manager at Lawrence Berkeley Lab when a 75-cent accounting error alerted him to the presence of an unauthorized user on his system. The hacker's code name was "Hunter"—a mysterious invader who managed to break into U.S. computer systems and steal sensitive military and security information. Stoll began a one-man hunt of his own: spying on the spy. It was a dangerous game of deception, broken codes, satellites, and missile bases—a one-man sting operation that finally gained the attention of the CIA . . . and ultimately trapped an international spy ring fueled by cash, cocaine, and the KGB.

El Jefe Alan Feuer 2020-08-25 The definitive account of the rise and fall of the ultimate narco, "El Chapo," from the New York Times reporter whose coverage of his trial went viral Joaquin “El Chapo” Guzman is the most legendary of Mexican narcos. As leader of the Sinaloa drug cartel, he was one of the most dangerous men in the world. His fearless climb to power, his brutality, his charm, his taste for luxury, his penchant for disguise, his multiple dramatic prison escapes, his unlikely encounter with Sean Penn—all of these burnished the image of the world's most famous outlaw. He was finally captured by U.S. and Mexican law enforcement in a daring operation years in the making. Here is that entire epic story—from El Chapo's humble origins to his conviction in a Brooklyn courthouse. Longtime New York Times criminal justice reporter Alan Feuer's coverage of his trial was some of the most riveting journalism of recent years. Feuer’s mastery of the complex facts of the case, his unparalleled access to confidential sources in law enforcement, and his powerful understanding of disturbing larger themes—what this one man's life says about drugs, walls, class, money, Mexico, and the United States—will

ensure that El Jefe is the one book to read about “El Chapo.”

Game Master: Mansion Mystery Rebecca Zamolo 2022-03-01 New York Times bestselling authors and creators of the mega-popular YouTube series Game Master Network Matt and Rebecca Zamolo return with a brand-new adventure about everyone’s favorite mystery-solving team. Rebecca Zamolo has managed to foil the Game Master’s plans before, but this time the Game Master has snake-napped Nacho, her good friend Miguel’s pet. No way is Becca going to let the Game Master get away with this dastardly plan. But when the clues lead Becca and her new friends in the direction of the one house in their entire neighborhood that none of them ever want to go near, they know they have no choice but to screw up their courage and dare to investigate, if they want to rescue Nacho. But the problem is that getting into the superspooky house is way easier than getting out. The Game Master is up to their old tricks, and Becca, Matt, Kylie, Frankie, and Miguel are going to have to face their fears and use all their smarts and strengths to solve the puzzles and games and save the day. Mansion Mystery is another action-packed adventure from New York Times bestselling authors and super-sleuthing team Rebecca and Matt Zamolo, stars of the hugely popular Game Master Network. Read the book and unlock special clues that will open exclusive content online!

Punisher Epic Collection Mike Baron 2019-02-06 Collecting Punisher (1987) #11-25 And Punisher Annual #1-2. Delivering justice from New York to Japan! Gary Saunders is on death row but the law doesn't move fast enough for the Punisher! The kids at Malcolm Shabazz High School had better behave for their new substitute teacher: Mr. Castle! But how does that lead to Frank trying to topple the Kingpin? He's determined to take down Wilson Fisk once and for all and it's all building to a brutal face-off! Then, Frank heads to Las Vegas in search of an assassin! A knockout round in the boxing ring leads to an encounter with the ninja Shadowmasters, and he'll team up with Moon Knight when Atlantis Attacks but what is the Punisher's part in the Evolutionary War? Plus: Frank takes on a war journal's worth of drug dealers, mobsters and criminals!

The Hacker Crackdown, Law and Disorder on the Electronic Frontier Bruce Sterling 2013-02 This book is part of the TREDITION CLASSICS. It contains classical literature works from over two thousand years. Most of these titles have been out of print and off the bookstore shelves for decades. The book series is intended to preserve the cultural legacy and to promote the timeless works of classical literature. Readers of a TREDITION CLASSICS book support the mission to save many of the amazing works of world literature from oblivion. With this series, tredition intends to make thousands of international literature classics available in printed format again - worldwide.

The Hacker Playbook 2 Peter Kim 2015-06-20 Just as a professional athlete doesn't show up without a solid game plan, ethical hackers, IT professionals, and security researchers should not be unprepared, either. The Hacker Playbook provides them their own game plans. Written by a longtime security professional

and CEO of Secure Planet, LLC, this step-by-step guide to the "game" of penetration hacking features hands-on examples and helpful advice from the top of the field. Through a series of football-style "plays," this straightforward guide gets to the root of many of the roadblocks people may face while penetration testing-including attacking different types of networks, pivoting through security controls, privilege escalation, and evading antivirus software. From "Pregame" research to "The Drive" and "The Lateral Pass," the practical plays listed can be read in order or referenced as needed. Either way, the valuable advice within will put you in the mindset of a penetration tester of a Fortune 500 company, regardless of your career or level of experience. This second version of The Hacker Playbook takes all the best "plays" from the original book and incorporates the latest attacks, tools, and lessons learned. Double the content compared to its predecessor, this guide further outlines building a lab, walks through test cases for attacks, and provides more customized code. Whether you're downing energy drinks while desperately looking for an exploit, or preparing for an exciting new job in IT security, this guide is an essential part of any ethical hacker's library-so there's no reason not to get in the game.

LEGO MINDSTORMS NXT James Floyd Kelly 2007-03-01 Through the use of a fictional story, this book details how to build and design robots. Max, the story's main character, is part of an archaeological expedition investigating a newly discovered Mayan pyramid. During the expedition, the team encounters various problems, each solved with the help of a unique robot that Max creates using the Lego Mindstorms NXT kit. Although the book reveals possible robotic solutions and offers detailed information on how to build and program each robot, readers are encouraged to come up with their own. The book includes complete building theory information and provides worksheets for brainstorming.

American Kingpin Nick Bilton 2017-05-02 NEW YORK TIMES BESTSELLER. The unbelievable true story of the man who built a billion-dollar online drug empire from his bedroom—and almost got away with it In 2011, a twenty-six-year-old libertarian programmer named Ross Ulbricht launched the ultimate free market: the Silk Road, a clandestine Web site hosted on the Dark Web where anyone could trade anything—drugs, hacking software, forged passports, counterfeit cash, poisons—free of the government’s watchful eye. It wasn’t long before the media got wind of the new Web site where anyone—not just teenagers and weed dealers but terrorists and black hat hackers—could buy and sell contraband detection-free. Spurred by a public outcry, the federal government launched an epic two-year manhunt for the site’s elusive proprietor, with no leads, no witnesses, and no clear jurisdiction. All the investigators knew was that whoever was running the site called himself the Dread Pirate Roberts. The Silk Road quickly ballooned into $1.2 billion enterprise, and Ross embraced his new role as kingpin. He enlisted a loyal crew of allies in high and low places, all as addicted to the danger and thrill of running an illegal marketplace as their customers were to the heroin they sold. Through his network he got wind of the target on his back and took drastic steps to protect himself—including ordering a hit on a former employee. As Ross made plans to disappear forever,

the Feds raced against the clock to catch a man they weren't sure even existed, searching for a needle in the haystack of the global Internet. Drawing on exclusive access to key players and two billion digital words and images Ross left behind, Vanity Fair correspondent and New York Times bestselling author Nick Bilton offers a tale filled with twists and turns, lucky breaks and unbelievable close calls. It's a story of the boy next door's ambition gone criminal, spurred on by the clash between the new world of libertarian-leaning, anonymous, decentralized Web advocates and the old world of government control, order, and the rule of law. Filled with unforgettable characters and capped by an astonishing climax, American Kingpin might be dismissed as too outrageous for fiction. But it's all too real.

Ethical Hacking Alana Maurushat 2019-04-09 How will governments and courts protect civil liberties in this new era of hacktivism? Ethical Hacking discusses the attendant moral and legal issues. The first part of the 21st century will likely go down in history as the era when ethical hackers opened governments and the line of transparency moved by force. One need only read the motto "we open governments" on the Twitter page for Wikileaks to gain a sense of the sea change that has occurred. Ethical hacking is the non-violent use of a technology in pursuit of a cause—political or otherwise—which is often legally and morally ambiguous. Hacktivists believe in two general but spirited principles: respect for human rights and fundamental freedoms, including freedom of expression and personal privacy; and the responsibility of government to be open, transparent and fully accountable to the public. How courts and governments will deal with hacking attempts which operate in a grey zone of the law and where different ethical views collide remains to be seen. What is undisputed is that Ethical Hacking presents a fundamental discussion of key societal questions. A fundamental discussion of key societal questions. This book is published in English. - La première moitié du XXIe siècle sera sans doute reconnue comme l'époque où le piratage éthique a ouvert de force les gouvernements, déplaçant les limites de la transparence. La page twitter de Wikileaks enchâsse cet ethos à même sa devise, « we open governments », et sa volonté d'être omniprésent. En parallèle, les grandes sociétés de technologie comme Apple se font compétition pour produire des produits de plus en plus sécuritaires et à protéger les données de leurs clients, alors même que les gouvernements tentent de limiter et de décrypter ces nouvelles technologies d'encryption. Entre-temps, le marché des vulnérabilités en matière de sécurité augmente à mesure que les experts en sécurité informatique vendent des vulnérabilités de logiciels des grandes technologies, dont Apple et Google, contre des sommes allant de 10 000 à 1,5 million de dollars. L'activisme en sécurité est à la hausse. Le piratage éthique est l'utilisation non-violence d'une technologie quelconque en soutien d'une cause politique ou autre qui est souvent ambigue d'un point de vue juridique et moral. Le hacking éthique peut désigner les actes de vérification de pénétration professionnelle ou d'experts en sécurité informatique, de même que d'autres formes d'actions émergentes, comme l'hacktivisme et la désobéissance civile en ligne. L'hacktivisme est une forme de piratage éthique, mais également une forme de militantisme des droits civils à l'ère numérique. En principe, les adeptes du hacktivisme croient en

deux grands principes : le respect des droits de la personne et les libertés fondamentales, y compris la liberté d'expression et à la vie privée, et la responsabilité des gouvernements d'être ouverts, transparents et pleinement redevables au public. En pratique, toutefois, les antécédents comme les agendas des hacktivistes sont fort diversifiés. Il n'est pas clair de quelle façon les tribunaux et les gouvernements traiteront des tentatives de piratage eu égard aux zones grises juridiques, aux approches éthiques conflictuelles, et compte tenu du fait qu'il n'existe actuellement, dans le monde, presque aucune exception aux provisions, en matière de cybercrime et de crime informatique, liées à la recherche sur la sécurité ou l'intérêt public. Il sera également difficile de déterminer le lien entre hacktivisme et droits civils. Ce livre est publié en anglais.

Spam Nation Brian Krebs 2014-11-18 Now a New York Times bestseller! There is a Threat Lurking Online with the Power to Destroy Your Finances, Steal Your Personal Data, and Endanger Your Life. In Spam Nation, investigative journalist and cybersecurity expert Brian Krebs unmasks the criminal masterminds driving some of the biggest spam and hacker operations targeting Americans and their bank accounts. Tracing the rise, fall, and alarming resurrection of the digital mafia behind the two largest spam pharmacies-and countless viruses, phishing, and spyware attacks-he delivers the first definitive narrative of the global spam problem and its threat to consumers everywhere. Blending cutting-edge research, investigative reporting, and firsthand interviews, this terrifying true story reveals how we unwittingly invite these digital thieves into our lives every day. From unassuming computer programmers right next door to digital mobsters like "Cosma"-who unleashed a massive malware attack that has stolen thousands of Americans' logins and passwords-Krebs uncovers the shocking lengths to which these people will go to profit from our data and our wallets. Not only are hundreds of thousands of Americans exposing themselves to fraud and dangerously toxic products from rogue online pharmacies, but even those who never open junk messages are at risk. As Krebs notes, spammers can-and do-hack into accounts through these emails, harvest personal information like usernames and passwords, and sell them on the digital black market. The fallout from this global epidemic doesn't just cost consumers and companies billions, it costs lives too. Fast-paced and utterly gripping, Spam Nation ultimately proposes concrete solutions for protecting ourselves online and stemming this tidal wave of cybercrime-before it's too late. "Krebs's talent for exposing the weaknesses in online security has earned him respect in the IT business and loathing among cybercriminals... His track record of scoops...has helped him become the rare blogger who supports himself on the strength of his reputation for hard-nosed reporting." -Bloomberg Businessweek

The Mastermind Evan Ratliff 2019-01-29 The incredible true story of the decade-long quest to bring down Paul Le Roux--the creator of a frighteningly powerful Internet-enabled cartel who merged the ruthlessness of a drug lord with the technological savvy of a Silicon Valley entrepreneur "Evan Ratliff has pried open a hidden world of high-tech gangsters and drug kingpins and double-crossers and stone-cold hitmen."--David Grann, author of Killers of the Flower

Moon It all started as an online prescription drug network, supplying hundreds of millions of dollars' worth of painkillers to American customers. It would not stop there. Before long, the business had turned into a sprawling multinational conglomerate engaged in almost every conceivable aspect of criminal mayhem. Yachts carrying $100 million in cocaine. Safe houses in Hong Kong filled with gold bars. Shipments of methamphetamine from North Korea. Weapons deals with Iran. Mercenary armies in Somalia. Teams of hit men in the Philippines. Encryption programs so advanced that the government could not break them. The man behind it all, pulling the strings from a laptop in Manila, was Paul Calder Le Roux--a reclusive programmer turned criminal genius who could only exist in the networked world of the twenty-first century, and the kind of self-made crime boss that American law enforcement had never imagined. For half a decade, DEA agents played a global game of cat-and-mouse with Le Roux as he left terror and chaos in his wake. Each time they came close, he would slip away. It would take relentless investigative work, and a shocking betrayal from within his organization, to catch him. And when he was finally caught, the story turned again, as Le Roux struck a deal to bring down his own organization and the people he had once employed. Award-winning investigative journalist Evan Ratliff spent four years piecing together this intricate puzzle, chasing Le Roux's empire and his shadowy henchmen around the world, conducting hundreds of interviews and uncovering thousands of documents. The result is a riveting, unprecedented account of a crime boss built by and for the digital age. Advance praise for The Mastermind "A true crime classic"--Publishers Weekly (starred review) "If truth is stranger than fiction, then The Mastermind is the truest book you'll read this year. The only thing predictable about it is how quickly you'll turn the pages."--Noah Hawley, author of Before the Fall and creator of the TV series Fargo

Breaking And Entering Jeremy N. Smith 2019-01-08 This taut, true thriller dives into a dark world that touches us all, as seen through the brilliant, breakneck career of an extraordinary hacker—a woman known only as Alien. When she arrived at MIT in the 1990s, Alien was quickly drawn to the school’s tradition of high-risk physical trespassing: the original “hacking.” Within a year, one of her hallmates was dead and two others were arraigned. Alien’s adventures were only just beginning. After a stint at the storied, secretive Los Alamos National Laboratory, Alien was recruited by a top cybersecurity firm where she deployed her cache of virtual weapons—and the trespassing and social engineering talents she had developed while “hacking” at MIT. The company tested its clients’ security by every means possible—not just coding, but donning disguises and sneaking past guards and secretaries into the C-suite. Alien now runs a boutique hacking outfit that caters to some of the world’s biggest and most vulnerable institutions—banks, retailers, government agencies. Her work combines devilish charm, old-school deception, and next generation spycraft. In Breaking and Entering, cybersecurity finally gets the rich, character-driven, fast-paced treatment it deserves.

Fatal System Error Joseph Menn 2010-10-26 In 2004, a California computer whiz named Barrett Lyon uncovered the identity of a hacker running major assaults on

business websites. Without fully grasping the repercussions, he set on an investigation that led him into the heart of the Russian mob. Cybercrime was evolving. No longer the domain of small-time thieves, it had been discovered by sophisticated gangs. They began by attacking corporate websites but increasingly stole financial data from consumers and defense secrets from governments. While Barrett investigated the cutting edge of technology crime, the U.S. government struggled to catch up. Britain, however, was a different story. In the late 1990s, the Queen herself had declared safe e-commerce a national security priority. Agents from the London-based National Hi-Tech Crime Unit sought out Barrett and enlisted his help. They also sent detective Andrew Crocker, a Welsh former boxer, to Russia to track down and prosecute the hackers -- and to find out who they worked for. Fatal System Error penetrates both the Russian cyber-mob and the American mafia as the two fight over the Internet's massive spoils. It takes readers into the murky hacker underground, traveling the globe from San Francisco to Costa Rica, London, and Russia. Using unprecedented access to mob businesses and Russian officials, it shows how top criminals earned protection from the Russian government -- and how Barrett Lyon and Andrew Crocker got closer to the titans of the underground economy than any previous outsider. Together, their stories explain why cybercrime is much worse than you thought -- and why the Internet might not survive.

Super Mario Jeff Ryan 2012-09-25 The definitive story of the rise of Nintendo. In 1981, Nintendo of America was a one-year-old business already on the brink of failure. Its president, Mino Arakawa, was stuck with two thousand unsold arcade cabinets for a dud of a game (Radar Scope). So he hatched a plan. Back in Japan, a boyish, shaggy-haired staff artist named Shigeru Miyamoto designed a new game for the unsold cabinets featuring an angry gorilla and a small jumping man. Donkey Kong brought in $180 million in its first year alone and launched the career of a short, chubby plumber named Mario. Since then, Mario has starred in over two hundred games, generating profits in the billions. He is more recognizable than Mickey Mouse, yet he’s little more than a mustache in bib overalls. How did a mere smear of pixels gain such huge popularity? Super Mario tells the story behind the Nintendo games millions of us grew up with, explaining how a Japanese trading card company rose to dominate the fiercely competitive video-game industry.

The Internet Police: How Crime Went Online, and the Cops Followed Nate Anderson 2013-08-19 A veteran reporter describes how authorities in Australia, Belgum, Ukraine and the United States combined forces to respond to a child pornography ring as well as how other criminal sting operations have been policed and patrolled online. 15,000 first printing.

The Fifth Domain Richard A. Clarke 2020-09-15 An urgent warning from two bestselling security experts--and a gripping inside look at how governments, firms, and ordinary citizens can confront and contain the tyrants, hackers, and criminals bent on turning the digital realm into a war zone. "In the battle raging between offense and defense in cyberspace, Clarke and Knake have some important ideas about how we can avoid cyberwar for our country, prevent

cybercrime against our companies, and in doing so, reduce resentment, division, and instability at home and abroad."--Bill Clinton There is much to fear in the dark corners of cyberspace: we have entered an age in which online threats carry real-world consequences. But we do not have to let autocrats and criminals run amok in the digital realm. We now know a great deal about how to make cyberspace far less dangerous--and about how to defend our security, economy, democracy, and privacy from cyber attack. Our guides to the fifth domain -- the Pentagon's term for cyberspace -- are two of America's top cybersecurity experts, seasoned practitioners who are as familiar with the White House Situation Room as they are with Fortune 500 boardrooms. Richard A. Clarke and Robert K. Knake offer a vivid, engrossing tour of the often unfamiliar terrain of cyberspace, introducing us to the scientists, executives, and public servants who have learned through hard experience how government agencies and private firms can fend off cyber threats. With a focus on solutions over scaremongering, and backed by decades of high-level experience in the White House and the private sector, The Fifth Domain delivers a riveting, agenda-setting insider look at what works in the struggle to avoid cyberwar.

Wrong Numbers Glen Meek 2019-10-15 Cybercrime meets organized crime in this true crime story about a hacker attempting to control Sin City’s call-girl racket. Was a hacker diverting phone calls meant for Las Vegas escort services? The FBI wanted to know, and so did associates of a New York Mafia family. In one of the most unusual undercover operations ever, the FBI had an agent acting as a manager in a real Las Vegas escort service. Federal agents expected to find prostitution and drugs in the Las Vegas escort industry. What their investigation uncovered was even more serious . . . Praise for Wrong Numbers “An intriguing and well-researched crime story detailing the intersection of big money and quick sex in the city that contains a lot of both.” —Jack Sheehan, author of Skin City “Wiseguys and wannabes are on the hunt for a shadowy hacker who may hold the keys to control of Las Vegas’ multi-million dollar call girl racket, while FBI agents are hunting them. The result is a gripping true-life crime story that reads like a collaboration between Elmore Leonard and William Gibson told with the knowing savvy of two longtime chroniclers of Sin City’s hidden underbelly.” —Kevin Poulsen, author of Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground “In ’90s Vegas, call girls worked for “entertainment” services that were little more than phone numbers, dispatchers, and drop safes. When a mystery hacker started diverting customers’ calls to one service’s number, it launched a series of dangerous events that involved the Mob, feds, hackers, service owners, and the phone system itself. This slice of Sin City history is as little-known as it is thrilling, and it’s well-told by investigative journalist Glen Meek and crime writer Dennis Griffin.” —Deke Castleman, author of Whale Hunt in the Desert: Secrets of a Vegas Superhost

Takedown Tsutomo Shimomura 1996-12-01 The dramatic true story of the capture of the world's most wanted cyberthief by brilliant computer expert Tsutomu Shimomura, describes Kevin Mitnick's long computer crime spree, which involved

millions of dollars in credit card numbers and corporate trade secrets. Reprint. NYT.

Future Crimes Marc Goodman 2015-02-24 NEW YORK TIMES and WALL STREET JOURNAL BESTSELLER ONE OF THE WASHINGTON POST'S 10 BEST BOOKS OF 2015 One of the world’s leading authorities on global security, Marc Goodman takes readers deep into the digital underground to expose the alarming ways criminals, corporations, and even countries are using new and emerging technologies against you—and how this makes everyone more vulnerable than ever imagined. Technological advances have benefited our world in immeasurable ways, but there is an ominous flip side: our technology can be turned against us. Hackers can activate baby monitors to spy on families, thieves are analyzing social media posts to plot home invasions, and stalkers are exploiting the GPS on smart phones to track their victims’ every move. We all know today’s criminals can steal identities, drain online bank accounts, and wipe out computer servers, but that’s just the beginning. To date, no computer has been created that could not be hacked—a sobering fact given our radical dependence on these machines for everything from our nation’s power grid to air traffic control to financial services. Yet, as ubiquitous as technology seems today, just over the horizon is a tidal wave of scientific progress that will leave our heads spinning. If today’s Internet is the size of a golf ball, tomorrow’s will be the size of the sun. Welcome to the Internet of Things, a living, breathing, global information grid where every physical object will be online. But with greater connections come greater risks. Implantable medical devices such as pacemakers can be hacked to deliver a lethal jolt of electricity and a car’s brakes can be disabled at high speed from miles away. Meanwhile, 3-D printers can produce AK-47s, bioterrorists can download the recipe for Spanish flu, and cartels are using fleets of drones to ferry drugs across borders. With explosive insights based upon a career in law enforcement and counterterrorism, Marc Goodman takes readers on a vivid journey through the darkest recesses of the Internet. Reading like science fiction, but based in science fact, Future Crimes explores how bad actors are primed to hijack the technologies of tomorrow, including robotics, synthetic biology, nanotechnology, virtual reality, and artificial intelligence. These fields hold the power to create a world of unprecedented abundance and prosperity. But the technological bedrock upon which we are building our common future is deeply unstable and, like a house of cards, can come crashing down at any moment. Future Crimes provides a mind-blowing glimpse into the dark side of technological innovation and the unintended consequences of our connected world. Goodman offers a way out with clear steps we must take to survive the progress unfolding before us. Provocative, thrilling, and ultimately empowering, Future Crimes will serve as an urgent call to action that shows how we can take back control over our own devices and harness technology’s tremendous power for the betterment of humanity—before it’s too late.

Becoming an Ethical Hacker Gary Rivlin 2019-05-07 An acclaimed investigative journalist explores ethical hacking and presents a reader-friendly, informative guide to everything there is to know about entering the field of cybersecurity.

It’s impossible to ignore the critical role cybersecurity plays within our society, politics, and the global order. In Becoming an Ethical Hacker, investigative reporter Gary Rivlin offers an easy-to-digest primer on what white hat hacking is, how it began, and where it’s going, while providing vivid case studies illustrating how to become one of these “white hats” who specializes in ensuring the security of an organization’s information systems. He shows how companies pay these specialists to break into their protected systems and networks to test and assess their security. Readers will learn how these white hats use their skills to improve security by exposing vulnerabilities before malicious hackers can detect and exploit them. Weaving practical how-to advice with inspiring case studies, Rivlin provides concrete, practical steps anyone can take to pursue a career in the growing field of cybersecurity.

Hacker, Hoaxer, Whistleblower, Spy Gabriella Coleman 2014-11-04 Here is the ultimate book on the worldwide movement of hackers, pranksters, and activists that operates under the non-name Anonymous, by the writer the Huffington Post says “knows all of Anonymous’ deepest, darkest secrets.” Half a dozen years ago, anthropologist Gabriella Coleman set out to study the rise of this global phenomenon just as some of its members were turning to political protest and dangerous disruption (before Anonymous shot to fame as a key player in the battles over WikiLeaks, the Arab Spring, and Occupy Wall Street). She ended up becoming so closely connected to Anonymous that the tricky story of her inside–outside status as Anon confidante, interpreter, and erstwhile mouthpiece forms one of the themes of this witty and entirely engrossing book. The narrative brims with details unearthed from within a notoriously mysterious subculture, whose semi-legendary tricksters—such as Topiary, tflow, Anachaos, and Sabu—emerge as complex, diverse, politically and culturally sophisticated people. Propelled by years of chats and encounters with a multitude of hackers, including imprisoned activist Jeremy Hammond and the double agent who helped put him away, Hector Monsegur, Hacker, Hoaxer, Whistleblower, Spy is filled with insights into the meaning of digital activism and little understood facets of culture in the Internet age, including the history of “trolling,” the ethics and metaphysics of hacking, and the origins and manifold meanings of “the lulz.”

Hardware Hacking Joe Grand 2004-01-29 "If I had this book 10 years ago, the FBI would never have found me!" -- Kevin Mitnick This book has something for everyone---from the beginner hobbyist with no electronics or coding experience to the self-proclaimed "gadget geek." Take an ordinary piece of equipment and turn it into a personal work of art. Build upon an existing idea to create something better. Have fun while voiding your warranty! Some of the hardware hacks in this book include: * Don't toss your iPod away when the battery dies! Don't pay Apple the $99 to replace it! Install a new iPod battery yourself without Apple's "help" * An Apple a day! Modify a standard Apple USB Mouse into a glowing UFO Mouse or build a FireWire terabyte hard drive and custom case * Have you played Atari today? Create an arcade-style Atari 5200 paddle controller for your favorite retro videogames or transform the Atari 2600

joystick into one that can be used by left-handed players * Modern game systems, too! Hack your PlayStation 2 to boot code from the memory card or modify your PlayStation 2 for homebrew game development * Videophiles unite! Design, build, and configure your own Windows- or Linux-based Home Theater PC * Ride the airwaves! Modify a wireless PCMCIA NIC to include an external antenna connector or load Linux onto your Access Point * Stick it to The Man! Remove the proprietary barcode encoding from your CueCat and turn it into a regular barcode reader * Hack your Palm! Upgrade the available RAM on your Palm m505 from 8MB to 16MB · Includes hacks of today's most popular gaming systems like Xbox and PS/2. · Teaches readers to unlock the full entertainment potential of their desktop PC. · Frees iMac owners to enhance the features they love and get rid of the ones they hate.

The Phoenix Project Gene Kim 2018-02-06 ***Over a half-million sold! The sequel, The Unicorn Project, is coming Nov 26*** “Every person involved in a failed IT project should be forced to read this book.”—TIM O’REILLY, Founder & CEO of O’Reilly Media “The Phoenix Project is a must read for business and IT executives who are struggling with the growing complexity of IT.”—JIM WHITEHURST, President and CEO, Red Hat, Inc. Five years after this sleeper hit took on the world of IT and flipped it on it's head, the 5th Anniversary Edition of The Phoenix Project continues to guide IT in the DevOps revolution. In this newly updated and expanded edition of the bestselling The Phoenix Project, co-author Gene Kim includes a new afterword and a deeper delve into the Three Ways as described in The DevOps Handbook. Bill, an IT manager at Parts Unlimited, has been tasked with taking on a project critical to the future of the business, code named Phoenix Project. But the project is massively over budget and behind schedule. The CEO demands Bill must fix the mess in ninety days or else Bill's entire department will be outsourced. With the help of a prospective board member and his mysterious philosophy of The Three Ways, Bill starts to see that IT work has more in common with a manufacturing plant work than he ever imagined. With the clock ticking, Bill must organize work flow streamline interdepartmental communications, and effectively serve the other business functions at Parts Unlimited. In a fast-paced and entertaining style, three luminaries of the DevOps movement deliver a story that anyone who works in IT will recognize. Readers will not only learn how to improve their own IT organizations, they'll never view IT the same way again. “This book is a gripping read that captures brilliantly the dilemmas that face companies which depend on IT, and offers real-world solutions.”—JEZ HUMBLE, Co-author of Continuous Delivery, Lean Enterprise, Accelerate, and The DevOps Handbook ——— “I’m delighted at how The Phoenix Project has reshaped so many conversations in technology. My goal in writing The Unicorn Project was to explore and reveal the necessary but invisible structures required to make developers (and all engineers) productive, and reveal the devastating effects of technical debt and complexity. I hope this book can create common ground for technology and business leaders to leave the past behind, and co-create a better future together.”—Gene Kim, November 2019

Think Like a Hacker Michael J. Melone 2017-06-27 Targeted attack and determined

human adversaries (DHA) have changed the information security game forever. Writing secure code is as important as ever; however, this satisfies only one piece of the puzzle. Effective defense against targeted attack requires IT professionals to understand how attackers use - and abuse - enterprise design to their advantage. Learn how advanced attackers break into networks. Understand how attackers use concepts of access and authorization to jump from one computer to the next. Dive into how and why attackers use custom implants and backdoors inside an enterprise. Be introduced to the concept of service-centric design - and how it can help improve both security and usability. To defend against hackers you must first learn to think like a hacker.

Freedom (TM) Daniel Suarez 2010-01-07 The New York Times bestseller Daemon unleashed a terrifying technological vision of an all-powerful, malicious computer program. Now, our world is the Daemon's world—unless someone stops it once and for all... The Daemon is in absolute control, using an expanded network of shadowy operatives to tear apart civilization and build it anew. Even as civil war breaks out in the American Midwest in a wave of nightmarish violence, former detective Pete Sebeck—the Daemon's most powerful, though reluctant, operative—must lead a small band of enlightened humans in a movement designed to protect the new world order. But the private armies of global business are preparing to crush the Daemon once and for all. In a world of shattered loyalties, collapsing societies, and seemingly endless betrayal, the only thing worth fighting for may be nothing less than the freedom of all humankind.

Kingpin Kevin Poulsen 2012 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.

Breakpoint Richard A. Clarke 2007-01-16 Air Force Combat Controller Dallas O'Halloran has a reputation as a hell-raising ladykiller. But he's also fiercely loyal. So when he's recruited by a new combat unit, Dallas is none too pleased to find himself teamed up with the icy blond JAG officer who nearly court-martialed his friends. Academy graduate Julianne Decatur is tough, tenacious, and driven by her belief in military law. She has zero patience for hot shot Spec-Ops cowboys who think the rules don't apply to them, and even less tolerance for Dallas' tough-as-nails Texas attitude. But when they're assigned to investigate a Navy flyer's apparent suicide, they discover the trail of a ruthless killer with a secret to hide—and an attraction between them that can't be denied. And when their prey turns the tables on them, Julianne will have to depend on the one man daring and reckless enough to keep them both alive.

100 Statements about Kingpin Daniel Palling 2013-01 In this book, we have hand-picked the most sophisticated, unanticipated, absorbing (if not at times crackpot!), original and musing book reviews of "Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground." Don't say we didn't warn you:

these reviews are known to shock with their unconventionality or intimacy. Some may be startled by their biting sincerity; others may be spellbound by their unbridled flights of fantasy. Don't buy this book if: 1. You don't have nerves of steel. 2. You expect to get pregnant in the next five minutes. 3. You've heard it all.

Kingpin Kevin Poulsen 2011-03-01 The true story of Max Butler, the master hacker who ran a billion dollar cyber crime network. The word spread through the hacking underground like some unstoppable new virus: an audacious crook had staged a hostile takeover of an online criminal network that siphoned billions of dollars from the US economy. The culprit was a brilliant programmer with a hippie ethic and a supervillain's double identity. Max 'Vision' Butler was a white-hat hacker and a celebrity throughout the programming world, even serving as a consultant to the FBI. But there was another side to Max. As the black-hat 'Iceman', he'd seen the fraudsters around him squabble, their ranks riddled with infiltrators, their methods inefficient, and in their dysfunction was the ultimate challenge: he would stage a coup and steal their ill-gotten gains from right under their noses. Through the story of Max Butler's remarkable rise, KINGPIN lays bare the workings of a silent crime wave affecting millions worldwide. It exposes vast online-fraud supermarkets stocked with credit card numbers, counterfeit cheques, hacked bank accounts and fake passports. Thanks to Kevin Poulsen's remarkable access to both cops and criminals, we step inside the quiet,desperate battle that law enforcement fights against these scammers. And learn that the boy next door may not be all he seems.

Silenced Paul Marshall 2011-11-17 This volume provides the first world survey of the range and effects of such accusations in the contemporary Muslim world, in international organizations, and in the West.

Industry of Anonymity Jonathan Lusthaus 2018-09-10 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.

Exploding the Phone Phil Lapsley 2013-02-05 “A rollicking history of the telephone system and the hackers who exploited its flaws.” —Kirkus Reviews, starred review Before smartphones, back even before the Internet and personal computers, a misfit group of technophiles, blind teenagers, hippies, and outlaws figured out how to hack the world’s largest machine: the telephone system. Starting with Alexander Graham Bell’s revolutionary “harmonic telegraph,” by the middle of the twentieth century the phone system had grown into something extraordinary, a web of cutting-edge switching machines and human operators that linked together millions of people like never before. But the network had a billion-dollar flaw, and once people discovered it, things would never be the same. Exploding the Phone tells this story in full for the first time. It traces the birth of long-distance communication and the

telephone, the rise of AT&T's monopoly, the creation of the sophisticated machines that made it all work, and the discovery of Ma Bell's Achilles' heel. Phil Lapsley expertly weaves together the clandestine underground of "phone phreaks" who turned the network into their electronic playground, the mobsters who exploited its flaws to avoid the feds, the explosion of telephone hacking in the counterculture, and the war between the phreaks, the phone company, and the FBI. The product of extensive original research, Exploding the Phone is a groundbreaking, captivating book that "does for the phone phreaks what Steven Levy's Hackers did for computer pioneers" (Boing Boing). "An authoritative, jaunty and enjoyable account of their sometimes comical, sometimes impressive and sometimes disquieting misdeeds." —The Wall Street Journal "Brilliantly researched." —The Atlantic "A fantastically fun romp through the world of early phone hackers, who sought free long distance, and in the end helped launch the computer era." —The Seattle Times

Worm Mark Bowden 2011-09-27 From the bestselling author of Black Hawk Down, the gripping story of the Conficker worm—the cyberattack that nearly toppled the world. The Conficker worm infected its first computer in November 2008, and within a month had infiltrated 1.5 million computers in 195 countries. Banks, telecommunications companies, and critical government networks—including British Parliament and the French and German military—became infected almost instantaneously. No one had ever seen anything like it. By January 2009, the worm lay hidden in at least eight million computers, and the botnet of linked computers it had created was big enough that an attack might crash the world. In this "masterpiece" (The Philadelphia Inquirer), Mark Bowden expertly lays out a spellbinding tale of how hackers, researchers, millionaire Internet entrepreneurs, and computer security experts found themselves drawn into a battle between those determined to exploit the Internet and those committed to protecting it.

The Hardware Hacker Andrew Bunnie Huang 2019-08-27 For over a decade, Andrew "bunnie" Huang, one of the world's most esteemed hackers, has shaped the fields of hacking and hardware, from his cult-classic book Hacking the Xbox to the open-source laptop Novena and his mentorship of various hardware startups and developers. In The Hardware Hacker, Huang shares his experiences in manufacturing and open hardware, creating an illuminating and compelling career retrospective. Huang's journey starts with his first visit to the staggering electronics markets in Shenzhen, with booths overflowing with capacitors, memory chips, voltmeters, and possibility. He shares how he navigated the overwhelming world of Chinese factories to bring chumby, Novena, and Chibitronics to life, covering everything from creating a Bill of Materials to choosing the factory to best fit his needs. Through this collection of personal essays and interviews on topics ranging from the legality of reverse engineering to a comparison of intellectual property practices between China and the United States, bunnie weaves engineering, law, and society into the tapestry of open hardware. With highly detailed passages on the ins and outs of manufacturing and a comprehensive take on the issues associated with open source hardware, The Hardware Hacker is an invaluable resource for aspiring

hackers and makers.

DarkMarket Misha Glenny 2011-10-04 "This extraordinarily powerful book demonstrates how utterly we lack the shared supranational tools needed to fight cybercrime. Essential reading." --Roberto Saviano, author of Gommorah The benefits of living in a digital, globalized society are enormous; so too are the dangers. The world has become a law enforcer’s nightmare and every criminal’s dream. We bank online; shop online; date, learn, work and live online. But have the institutions that keep us safe on the streets learned to protect us in the burgeoning digital world? Have we become complacent about our personal security—sharing our thoughts, beliefs and the details of our daily lives with anyone who might care to relieve us of them? In this fascinating and compelling book, Misha Glenny, author of the international best seller McMafia, explores the three fundamental threats facing us in the twenty-first century: cybercrime, cyberwarfare and cyberindustrial espionage. Governments and the private sector are losing billions of dollars each year fighting an ever-morphing, often invisible and often supersmart new breed of criminal: the hacker. Glenny has traveled and trawled the world. By exploring the rise and fall of the criminal website DarkMarket he has uncovered the most vivid, alarming and illuminating stories. Whether JiLsi or Matrix, Iceman, Master Splynter or Lord Cyric; whether Detective Sergeant Chris Dawson in Scunthorpe, England, or Agent Keith Mularski in Pittsburgh, Pennsylvania, Glenny has tracked down and interviewed all the players—the criminals, the geeks, the police, the security experts and the victims—and he places everyone and everything in a rich brew of politics, economics and history. The result is simply unputdownable. DarkMarket is authoritative and completely engrossing. It’s a must-read for everyone who uses a computer: the essential crime book for our times.