Spam Nation The Inside Story Of Organized Cybercrime From Global Epidemic To Your Front Door

In 2014, College Board rolled out a new AP® U.S. History course, which centered less on memorizing content and more on developing skills. Since then, the course has been modified here and there, but very little has changed in AP® textbooks--content is still king. Until now. Fabric of a Nation is the first book to truly embrace this dramatic shift in the AP® course and in how history is taught. Built from the ground up by long-time AP® leaders Jason Stacy and Matthew Ellington, this book offers a new approach to AP® US History by seamlessly integrating: A brief historical narrative AP® skills practice Primary source documents Exact alignment to the AP® course Now, that's revolutionary!

When a giant wave destroys his village, Mau is the only one left. Daphne—a traveler from the other side of the globe—is the sole survivor of a shipwreck. Separated by language and customs, the two are united by catastrophe. Slowly, they are joined by other refugees. And as they struggle to protect the small band, Mau and Daphne defy ancestral spirits, challenge death himself, and uncover a long-hidden secret that literally turns the world upside down.

Choosing the right people to carry out a project is essential to its success. When multiple projects are combined into a complex program, the human aspect becomes even more important. This book is the first to truly balance a complete account of the technical aspects of project and program management with a practical approach to understanding and developing the core competencies required to accomplish desired goals. On the technical side, this book is a complete introduction to predicting costs, setting schedules, and assessing risks. On the people side, it sheds new light on how to mold different personality types into a team, how to motivate the team's members, and how to produce extraordinary results. The author details the essential parts of the program management approach, describing the best way to define, organize, and schedule the work to be done, identifying risks and controlling costs during the whole process. This fourth edition has been significantly revised, with every chapter updated. The volume considers the magnitude of recent social, political, and technological changes, and the impact is represented throughout this book. Included are insights from numerous students who bring to the forefront their current real-world practices from their individual businesses, industries, and disciplines.

With the rise of surveillance technology in the last decade, police departments now have an array of sophisticated tools for tracking, monitoring, even predicting crime patterns. In particular crime mapping, a technique used by the police to monitor crime by the neighborhoods in their geographic regions, has become a regular and relied-upon feature of policing. Many claim that these technological developments played a role in the crime drop of the 1990s, and yet no study of these techniques and their relationship to everyday police work has been made available. Noted scholar Peter K. Manning spent six years observing three American police departments and two British constabularies in order to determine what effects these kinds of analytic tools have had on modern police management and practices. While modern technology allows the police to combat crime in sophisticated, detail-oriented ways, Manning discovers that police strategies and tactics have not been altogether transformed as perhaps would be expected. In The Technology of Policing, Manning untangles the varying kinds of complex crime-control rhetoric that underlie much of today ' s police department discussion and management, and provides valuable insight into which are the most effective—and which may be harmful—in successfully tracking criminal behavior. The Technology of Policing offers a new understanding of the changing world of police departments and information technology ' s significant and undeniable influence on crime management.

Simple Strategies to Outsmart Today's Rip-off Artists

Countdown to Zero Day

Click Here to Kill Everybody: Security and Survival in a Hyper-connected World

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

Spam Kings

Crime Dot Com

Social Networks and the Death of Privacy

Cyberpunk

Written by experts on the frontlines, Investigating Internet Crimes provides seasoned and new investigators with the background and tools they need to investigate crime occurring in the online world. This invaluable guide provides step-by-step instructions for investigating Internet crimes, including locating, interpreting, understanding, collecting, and documenting online electronic evidence to benefit investigations. Cybercrime is the fastest growing area of crime as more criminals seek to exploit the speed, convenience and anonymity that the Internet provides to commit a diverse range of criminal activities. Today's online crime includes attacks against computer data and systems, identity theft, distribution of child pornography, penetration of online financial services, using social networks to commit crimes, and the deployment of viruses, botnets, and email scams such as phishing. Symantec's 2012 Norton Cybercrime Report stated that the world spent an estimated $110 billion to combat cybercrime, an average of nearly $200 per victim. Law enforcement agencies and corporate security officers around the world with the responsibility for enforcing, investigating and prosecuting cybercrime are overwhelmed, not only by the sheer number of crimes being committed but by a lack of adequate training material. This book provides that fundamental knowledge, including how to properly collect and document online evidence, trace IP addresses, and work undercover. Provides step-by-step instructions on how to investigate crimes online Covers how new software tools can assist in online investigations Discusses how to track down, interpret, and understand online electronic evidence to benefit investigations Details guidelines for collecting and documenting online evidence that can be presented in court

This is an exciting new edition of a core textbook that explores innovation management from a global perspective. Innovation management is increasingly significant, both as an academic discipline and as an integral part of the way businesses seek to change and grow. However the key factors behind successful innovation and the process by which innovation is turned into profit in the global arena remain largely undefined. The new edition provides a unique answer to these questions and offers a step-by-step guide to innovation strategy development, taking into account the global context in which businesses today operate. Written by a highly experienced instructor, this is an ideal companion for undergraduate students of innovation as well as postgraduate and MBA students taking modules with an innovation component. New to this Edition: - Completely rewritten and restructured to explore in more depth how innovative ideas are identified and strategized in an increasingly globalized world - Fully updated and extended case studies on world-leading companies - Increased attention to commercialized innovation, including factors such as intellectual property laws, technology acceleration and the competition for venture capital and finance - Coverage of new topics such as open innovation and service innovation - Expanded coverage of the tools and methods needed to understand financial gain and risk

New York Times Notable Book: "A well-told business yarn . . . A fly-on-the-wall look at how eBay got to be eBay." —Chicago Tribune When Pierre Omidyar launched a clunky website from a spare bedroom over Labor Day weekend of 1995, he wanted to see if he could use the Internet to create a perfect market. He never guessed his old-computer parts and Beanie Baby exchange would revolutionize the world of commerce. In this fascinating book, Adam Cohen, the first journalist ever to get full access to the company, tells the remarkable story of eBay's rise. He describes how eBay built the most passionate community ever to form in cyberspace and forged a business that triumphed over larger, better-funded rivals. And he explores the ever-widening array of enlistees in the eBay revolution, from a stay-at-home mom who had to rent a warehouse for her thriving business selling bubble-wrap on eBay to the young MBA who started eBay Motors (which within months of its launch was on track to sell $1 billion in cars a year), to collectors nervously bidding thousands of dollars on antique clothing-irons. "Skillfully synthesizes the story of eBay's corporate evolution with profiles of more peripheral figures." —The Washington Post Book World "The definitive history of eBay—a strange and exhilarating tale." —Jeffrey Toobin, New York Times-bestselling author of True Crimes and Misdemeanors

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.

Dark Commerce

CyberThieves, CyberCops and You

Grime Kids

The SAGE Encyclopedia of Surveillance, Security, and Privacy

Outlaws and Hackers on the Computer Frontier, Revised

The Inside Story of the Global Grime Takeover

Solving Cyber Risk

I Know Who You Are and I Saw What You Did

"A memoir from Ta-Nehisi Coates, in which he details the challenges on the streets and within one's family, especially the eternal struggle for peace between a father and son and the important role family plays in such circumstances"--

"People are stupid, Davis Wolfgang Hawke thought as he stared at the nearly empty box of Swastika pendants on his desk." So begins Spam Kings, an investigative look into the shady world of email spammers and the people trying to stop them. This compelling exposé explores the shadowy world of the people responsible for today's junk-email epidemic. Investigative journalist Brian McWilliams delivers a fascinating account of the cat-and-mouse game played by spam entrepreneurs in search of easy fortunes and anti-spam activists. McWilliams chronicles the activities of several spam kings, including Hawke, a notorious Jewish-born neo-Nazi leader. You'll follow this 20-year-old's rise in the trade, where he became a major player in the lucrative penis pill market—a business that would make him a millionaire and the target of lawsuits. You'll also meet cyber-vigilantes, such as Susan Gunn, who have taken up the fight against spammers like Hawke. Explore the sleazy spammer business practices, the surprising new partnership between spammers and computer hackers, and the rise of a new breed of computer viruses designed to turn the PCs of innocent bystanders into secret spam factories.

Profiles computer hackers who overstep ethical boundaries and break the law to penetrate society's most sensitive computer networks.

This dazzling Christmas poem by Maya Angelou is powerful and inspiring for people of all faiths. In this beautiful, deeply moving poem, Maya Angelou inspires us to embrace the peace and promise of Christmas, so that hope and love can once again light up our holidays and the world. "Angels and Mortals, Believers and Nonbelievers, look heavenward," she writes, "and speak the word aloud. Peace." Read by the poet at the lighting of the National Christmas Tree at the White House on December 1, 2005, Maya Angelou' s celebration of the "Glad Season" is a radiant affirmation of the goodness of life.

Correlates, Causes, and Context

Amazing Peace

The Technology of Policing

The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door

The Art of Intrusion

Spam Nation

An Oral History as Told by Jon Stewart, the Correspondents, Staff and Guests

Inside Ebay

NEW YORK TIMES BESTSELLER WASHINGTON POST BESTSELLER Winner of the getAbstract 17th International Book Award "The Seventh Sense is a concept every businessman, diplomat, or student should aspire to master--a powerful idea, backed by stories and figures that will be impossible to forget." -- Walter Isaacson, author of Steve Jobs and Leonardo da Vinci Endless terror. Refugee waves. An unfixable global economy. Surprising election results. New billion-dollar fortunes. Miracle medical advances. What if they were all connected? What if you could understand why? The Seventh Sense is the story of what all of today's successful figures see and feel: the forces that are invisible to most of us but explain everything from explosive technological change to uneasy political ripples. The secret to power now is understanding our new age of networks. Not merely the Internet, but also webs of trade, finance, and even DNA. Based on his years of advising generals, CEOs, and politicians, Ramo takes us into the opaque heart of our world's rapidly connected systems and teaches us what the losers are not yet seeing--and what the victors of this age already know.

Top cybersecurity journalist Kim Zetter tells the story behind the virus that sabotaged Iran's nuclear efforts and shows how its existence has ushered in a new age of warfare—one in which a digital attack can have the same destructive capability as a megaton bomb. In January 2010, inspectors with the International Atomic Energy Agency noticed that centrifuges at an Iranian uranium enrichment plant were failing at an unprecedented rate. The cause was a complete mystery—apparently as much to the technicians replacing the centrifuges as to the inspectors observing them. Then, five months later, a seemingly unrelated event occurred: A computer security firm in Belarus was called in to troubleshoot some computers in Iran that were crashing and rebooting repeatedly. At first, the firm's programmers believed the malicious code on the machines was a simple, routine piece of malware. But as they and other experts around the world investigated, they discovered a mysterious virus of unparalleled complexity. They had, they soon learned, stumbled upon the world's first digital weapon. For Stuxnet, as it came to be known, was unlike any other virus or worm built before: Rather than simply hijacking targeted computers or stealing information from them, it escaped the digital realm to wreak actual, physical destruction on a nuclear facility. In these pages, Wired journalist Kim Zetter draws on her extensive sources and expertise to tell the story behind Stuxnet's planning, execution, and discovery, covering its genesis in the corridors of Bush's White House and its unleashing on systems in Iran—and telling the spectacular, unlikely tale of the security geeks who managed to unravel a sabotage campaign years in the making. But Countdown to Zero Day ranges far beyond Stuxnet itself. Here, Zetter shows us how digital warfare developed in the US. She takes us inside today's flourishing zero-day "grey markets," in which intelligence agencies and militaries pay huge sums for the malicious code they need to carry out infiltrations and attacks. She reveals just how vulnerable many of our own critical systems are to Stuxnet-like strikes, from nation-state adversaries and anonymous hackers alike—and shows us just what might happen should our infrastructure be targeted by such an attack. Propelled by Zetter's unique knowledge and access, and filled with eye-opening explanations of the technologies involved, Countdown to Zero Day is a comprehensive and prescient portrait of a world at the edge of a new kind of war.

As research continues to accumulate on the connections between media and crime, #Crime explores the impact of social media on the criminal legal system. It examines how media influences our perceptions of crime, the perpetration of crime, and the implementation of punishment, whilst emphasizing the significance of race, ethnicity, class, gender, and sexuality. It offers an accessible and in-depth examination of media and in each chapter there are case studies and examples from both legacy and new media, including discussions from Twitter that are being used to raise awareness of criminal legal issues. It also includes interviews with international scholars and practitioners from Australia, Belgium, and the United States to voice a range of global perspectives. This book speaks broadly to those interested in criminology, criminal justice, media and culture, sociology, and gender studies.

Hacker extraordinaire Kevin Mitnick delivers the explosive encore to his bestselling The Art of Deception Kevin Mitnick, the world's most celebrated hacker, now devotes his life to helping businesses and governments combat data thieves, cybervandals, and other malicious computer intruders. In his bestselling The Art of Deception, Mitnick presented fictionalized case studies that illustrated how savvy computer crackers use "social engineering" to compromise even the most technically secure computer systems. Now, in his new book, Mitnick goes one step further, offering hair-raising stories of real-life computer break-ins-and showing how the victims could have prevented them. Mitnick's reputation within the hacker community gave him unique credibility with the perpetrators of these crimes, who freely shared their stories with him-and whose exploits Mitnick now reveals in detail for the first time, including: A group of friends who won nearly a million dollars in Las Vegas by reverse-engineering slot machines Two teenagers who were persuaded by terrorists to hack into the Lockheed Martin computer systems Two convicts who joined forces to become hackers inside a Texas prison A "Robin Hood" hacker who penetrated the computer systems of many prominent companies-andthen told them how he gained access With riveting "you are there" descriptions of real computer break-ins, indispensable tips on countermeasures security professionals need to implement now, and Mitnick's own acerbic commentary on the crimes he describes, this book is sure to reach a wide audience-and attract the attention of both law enforcement agencies and the media.

Global Innovation Management

Fabric of a Nation

Why Don't You Like Me?

A Competency-Based Approach

Industry of Anonymity

From Viruses to Vote Rigging, How Hacking Went Global

Automate This

The Real Story Behind the High-Rolling Hucksters Pushing Porn, Pills, and %*@)# Enlargements

A world of "smart" devices means the Internet can kill people. We need to act. Now. Everything is a computer. Ovens are computers that make things hot; refrigerators are computers that keep things cold. These computers—from home thermostats to chemical plants—are all online. The Internet, once a virtual abstraction, can now sense and touch the physical world. As we open our lives to this future, often called the Internet of Things, we are beginning to see its enormous potential in ideas like driverless cars, smart cities, and personal agents equipped with their own behavioral algorithms. But every knife cuts two ways. All computers can be hacked. And Internet-connected computers are the most vulnerable. Forget data theft: cutting-edge digital attackers can now crash your car, your pacemaker, and the nation's power grid. In Click Here to Kill Everybody, renowned expert and best-selling author Bruce Schneier examines the hidden risks of this new reality. After exploring the full implications of a world populated by hyperconnected devices, Schneier reveals the hidden web of technical, political, and market forces that underpin the pervasive insecurities of today. He then offers common-sense choices for companies, governments, and individuals that can allow us to enjoy the benefits of this omnipotent age without falling prey to its vulnerabilities. From principles for a more resilient Internet of Things, to a recipe for sane government regulation and oversight, to a better way to understand a truly new environment, Schneier's vision is required reading for anyone invested in human flourishing.

As David Cameron's director of Politics and communications, Craig Oliver was in the room at every key moment during the EU referendum - the biggest political event in the UK since World War 2. Craig Oliver worked with all the players, including David Cameron, George Osbourne, Barack Obama, Angela Merkel, Jeremy Corbyn, Boris Johnson,Michael Gove, Theresa May and Peter Mandelson. Unleashing Demons is based on his extensive notes, detailing everything from the decision to call a referendum, to the subsequent civil war in the Conservative Party and the aftermath of the shocking result. This is raw history at its very best, packed with enthralling detail and colourful anecdotes from behind the closed doors of the campaign that changed British history.

"This book uncovers and explains how surveillance has come to be an integral part of how our contemporary society operates worldwide and how it impacts our security and privacy. It explores all types of surveillance, including political, security, corporate, and economic, at all levels of social structure, from the personal to the political to the economic to the judicial."--

Shortlisted for the Orwell Prize and the CWA Gold Dagger for Non-Fiction Award The benefits of living in a digital, globalised 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 cares to relieve us of them? In this fascinating and compelling book, Misha Glenny, author of the international bestseller McMafia, explores the three fundamental threats facing us in the twenty-first century: cyber crime, cyber warfare and cyber industrial espionage. Governments and the private sector are losing billions of dollars each year, fighting an ever-morphing, often invisible, and highly intelligent new breed of criminal: the hacker. Glenny has travelled and trawled the world. And 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 Bolton or Agent Keith Mularski in Pittsburgh, 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.

Proactive Cybersecurity Strategies for Today's Leaders

How a New Illicit Economy Is Threatening Our Future

CUCKOO'S EGG

The Beautiful Struggle (Adapted for Young Adults)

Crime Mapping, Information Technology, and the Rationality of Crime Control

Beautiful Security

Project and Program Management

Protecting Your Company and Society

Organizations around the world are in a struggle for survival, racing to transform themselves in a herculean effort to adapt to the digital age, all while protecting themselves from headline-grabbing cybersecurity threats. As organizations succeed or fail, the centrality and importance of cybersecurity and the role of the CISO—Chief Information Security Officer—becomes ever more apparent. It's becoming clear that the CISO, which began as a largely technical role, has become nuanced, strategic, and a cross-functional leadership position. Fight Fire with Fire: Proactive Cybersecurity Strategies for Today's Leaders explores the evolution of the CISO's responsibilities and delivers a blueprint to effectively improve cybersecurity across an organization. Fight Fire with Fire draws on the deep experience of its many all-star contributors. For example: Learn how to talk effectively with the Board from engineer-turned-executive Marianne Bailey, a top spokesperson well-known for global leadership in cyber Discover how to manage complex cyber supply chain risk with Terry Roberts, who addresses this complex area using cutting-edge technology and emerging standards Tame the exploding IoT threat landscape with Sonia Arista, a CISO with decades of experience across sectors, including healthcare where edge devices monitor vital signs and robots perform surgery These are just a few of the global trailblazers in cybersecurity who have banded together to equip today's leaders to protect their enterprises and inspire tomorrow's leaders to join them. With fires blazing on the horizon, there is no time for a seminar or boot camp. Cyber leaders need information at their fingertips. Readers will find insight on how to close the diversity and skills gap and become well-versed in modern cyber threats, including attacks coming from organized crime and nation-states. This book highlights a three-pronged approach that encompasses people, process, and technology to empower everyone to protect their organization. From effective risk management to supply chain security and communicating with the board, Fight Fire with Fire presents discussions from industry leaders that cover every critical competency in information security. Perfect for IT and information security professionals seeking perspectives and insights they can't find in certification exams or standard textbooks, Fight Fire with Fire is an indispensable resource for everyone hoping to improve their understanding of the realities of modern cybersecurity through the eyes of today's top security leaders.

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.

According to the World Health Organization: The UK is the second most obese nation on the planet [the US is the first]. One in five British adults is obese Two-thirds of men and half of women are overweight 31,000 British deaths a year are obesity-related Obesity costs 500 million to the NHS and 2 billion to the economy each year.Yet health and fitness clubs are booming, with 6 million members in Britain, while millions more are dieting. The Hungry Gene takes an unflinching look at the spread of obesity, the most vexing scientific mysteries of our time.Acclaimed science journalist Ellen Ruppel Shell reveals the existence of a gene that causes obesity and meets the scientists working to isolate it. She looks at how medicine is dealing with the fat crisis with radical surgical techniques and takes aim at the culture behind the crisis - suburban sedentary lifestyle and the fast-food market that preys on the jammed schedules of today's two-income families.Weaving cutting-edge science, history and personal stories, the narrative builds to a powerful conclusion that reveals how we can beat obesity before it flattens us. Gripping and provocative, The Hungry Gene is the unsettling account of how the western world got fat - and what we can do about it.

An explosive insider account of grime, from subculture to international phenomenon. ***** A group of kids in the 2000s had a dream to make their voice heard - and this book documents their seminal impact on today's pop culture. DJ Target grew up in Bow under the shadow of Canary Wharf, with money looming close on the skyline. The 'Godfather of Grime' Wiley and Dizzee Rascal first met each other in his bedroom. They were all just grime kids on the block back then, and didn't realise they were to become pioneers of an international music revolution. A movement that permeates deep into British culture and beyond. Household names were borne out of those housing estates, and the music industry now jumps to the beat of their gritty reality rather than the tune of glossy aspiration. Grime has shaken the world and Target is revealing its explosive and expansive journey in full, using his own unique insight and drawing on the input of grime's greatest names.

Investigating Internet Crimes

The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers

Building an Effective Security Program

A Christmas Poem

Leading Security Experts Explain How They Think

Introduction to Probability

How Algorithms Took Over Our Markets, Our Jobs, and the World

Are you at risk of being scammed? Former con artist and bestselling author of Catch Me If You Can Frank Abagnale shows you how to stop scammers in their tracks. Maybe you're wondering how to make the scam phone calls stop. Perhaps someone has stolen your credit card number. Or you've been a victim of identity theft. Even if you haven't yet been the target of a crime, con artists are always out there, waiting for the right moment to steal your information, your money, and your life. As one of the world's most respected authorities on the subjects of fraud, forgery, and cyber security, Frank Abagnale knows how scammers work. In Scam Me If You Can, he reveals the latest tricks that today's scammers, hackers, and con artists use to steal your money and personal information--often online and over the phone. Using plain language and vivid examples, Abagnale reveals hundreds of tips, including: • The best way to protect your phone from being hacked • The only time you should ever use a debit card • The one type of photo you should never post on social media • The only conditions under which you should use WiFi networks at the airport • The safest way to use an ATM With his simple but counterintuitive rules, Abagnale also makes use of his insider intel to paint a picture of cybercrimes that haven't become widespread yet.

Developed from celebrated Harvard statistics lectures, Introduction to Probability provides essential language and tools for understanding statistics, randomness, and uncertainty. The book explores a wide variety of applications and examples, ranging from coincidences and paradoxes to Google PageRank and Markov chain Monte Carlo (MCMC). Additional

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

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.

DarkMarket

The Seventh Sense

The Hungry Gene

Power, Fortune, and Survival in the Age of Networks

Scam Me If You Can

A Brief History with Skills and Sources, For the AP® Course

Crime Online

The Inside Story of Brexit

Spam NationThe Inside Story of Organized Cybercrime-from Global Epidemic to Your Front DoorSourcebooks, Inc.

Although most people don't give security much attention until their personal or business systems are attacked, this thought-provoking anthology demonstrates that digital security is not only worth thinking about, it's also a fascinating topic. Criminals succeed by exercising enormous creativity, and those defending against them must do the same. Beautiful Security explores this challenging subject with insightful essays and analysis on topics that include: The underground economy for personal information: how it works, the relationships among criminals, and some of the new ways they pounce on their prey How social networking, cloud computing, and other popular trends help or hurt our online security How metrics, requirements gathering, design, and law can take security to a higher level The real, little-publicized history of PGP This book includes contributions from: Peiter "Mudge" Zatko Jim Stickley Elizabeth Nichols Chenxi Wang Ed Bellis Ben Edelman Phil Zimmermann and Jon Callas Kathy Wang Mark Curphey John McManus James Routh Randy V. Sabett Anton Chuvakin Grant Geyer and Brian Dunphy Peter Wayner Michael Wood and Fernando Francisco All royalties will be donated to the Internet Engineering Task Force (IETF).

A comprehensive look at the world of illicit trade Though mankind has traded tangible goods for millennia, recent technology has changed the fundamentals of trade, in both legitimate and illegal economies. In the past three decades, the most advanced forms of illicit trade have broken with all historical precedents and, as Dark Commerce shows, now operate as if on steroids, tied to computers and social media. In this new world of illicit commerce, which benefits states and diverse participants, trade is impersonal and anonymized, and vast profits are made in short periods with limited accountability to sellers, intermediaries, and purchasers. Louise Shelley examines how new technology, communications, and globalization fuel the exponential growth of dangerous forms of illegal trade—the markets for narcotics and child pornography online, the escalation of sex trafficking through web advertisements, and the sale of endangered species for which revenues total in the hundreds of millions of dollars. The illicit economy exacerbates many of the world's destabilizing phenomena: the perpetuation of conflicts, the proliferation of arms and weapons of mass destruction, and environmental degradation and extinction. Shelley explores illicit trade in tangible goods—drugs, human beings, arms, wildlife and timber, fish, antiquities, and ubiquitous counterfeits—and contrasts this with the damaging trade in cyberspace, where intangible commodities cost consumers and organizations billions as they lose identities, bank accounts, access to computer data, and intellectual property. Demonstrating that illicit trade is a business the global community cannot afford to ignore and must work together to address, Dark Commerce considers diverse ways of responding to this increasing challenge.

Hailed as "stunning" (New York Post), "authoritative" (Kirkus Reviews), and "comprehensively researched" (Shelf Awareness), a shocking exposé of the widespread abuses of our personal online data by a leading specialist on Web privacy. Social networks, the defining cultural movement of our time, offer many freedoms. But as we work and shop and date over the Web, we are opening ourselves up to intrusive privacy violations by employers, the police, and aggressive data collection companies that sell our information to any and all takers. Through groundbreaking research, Andrews reveals how routinely colleges reject applicants due to personal information searches, robbers use vacation postings to target homes for break-ins, and lawyers scour our social media for information to use against us in court. And the legal system isn't protecting us—in the thousands of privacy violations brought to trial, judges often rule against the victims. Providing expert advice and leading the charge to secure our rights, Andrews proposes a Social Network Constitution to protect us all. Now is the time to join her and take action—the very future of privacy is at stake. Log on to www.loriandrews.com to sign the Constitution for Web Privacy.

Unleashing Demons

Kingpin

How One Hacker Took Over the Billion-Dollar Cybercrime Underground

Social Media, Crime, and the Criminal Legal System

#Crime

The Perfect Store

Future Crimes

The Science of Fat and the Future of Thin

The rousing story of the last gasp of human agency and how today's best and brightest minds are endeavoring to put an end to it. It used to be that to diagnose an illness, interpret legal documents, analyze foreign policy, or write a newspaper article you needed a human being with specific skills—and maybe an advanced degree or two. These days, high-level tasks are increasingly being handled by algorithms that can do precise work not only with speed but also with nuance. These "bots" started with human programming and logic, but now their reach extends beyond what their creators ever expected. In this fascinating, frightening book, Christopher Steiner tells the story of how algorithms took over—and shows why the "bot revolution" is about to spill into every aspect of our lives, often silently, without our knowledge. The May 2010 "Flash Crash" exposed Wall Street's reliance on trading bots to the tune of a 998-point market drop and $1 trillion in vanished market value. But that was just the beginning. In Automate This, we meet bots that are driving cars, penning haiku, and writing music mistaken for Bach's. They listen in on our customer service calls and figure out what Iran would do in the event of a nuclear standoff. There are algorithms that can pick out the most cohesive crew of astronauts for a space mission or identify the next Jeremy Lin. Some can even ingest statistics from baseball games and spit out pitch-perfect sports journalism indistinguishable from that produced by humans. The interaction of man and machine can make our lives easier. But what will the world look like when algorithms control our hospitals, our roads, our culture, and our national security? What happens to businesses when we automate judgment and eliminate human instinct? And what role will be left for doctors, lawyers, writers, truck drivers, and many others? Who knows—maybe there's a bot learning to do your job this minute.

The non-technical handbook for cyber security risk management Solving Cyber Risk distills a decade of research into a practical framework for cyber security. Blending statistical data and cost information with research into the culture, psychology, and business models of the hacker community, this book provides business executives, policy-makers, and individuals with a deeper understanding of existing future threats, and an action plan for safeguarding their organizations. Key Risk Indicators reveal vulnerabilities based on organization type, IT infrastructure and existing security measures, while expert discussion from leading cyber risk specialists details practical, real-world methods of risk reduction and mitigation. By the nature of the business, your organization's customer database is packed with highly sensitive information that is essentially hacker-bait, and even a minor flaw in security protocol could spell disaster. This book takes you deep into the cyber threat landscape to show you how to keep your data secure. Understand who is carrying out cyber-attacks, and why Identify your organization's risk of attack and vulnerability to damage Learn the most cost-effective risk reduction measures Adopt a new cyber risk assessment and quantification framework based on techniques used by the insurance industry By applying risk management principles to cyber security, non-technical leadership gains a greater understanding of the types of threat, level of threat, and level of investment needed to fortify the organization against attack. Just because you have not been hit does not mean your data is safe, and hackers rely on their targets' complacence to help maximize their haul. Solving Cyber Risk gives you a concrete action plan for implementing top-notch preventative measures before you're forced to implement damage control.

"Brilliantly researched and written."—Jon Snow, Channel 4 News "A comprehensive and intelligible account of the elusive world of hacking and cybercrime over the last two decades. . . . Lively, insightful, and, often, alarming."—Ewen MacAskill, Guardian On May 4, 2000, an email that read "kindly check the attached LOVELETTER" was sent from a computer in the Philippines. Attached was a virus, the Love Bug, and within days it had been circulated across the globe, paralyzing banks, broadcasters, and businesses in its wake, and extending as far as the UK Parliament and, reportedly, the Pentagon. The outbreak presaged a new era of online mayhem: the age of Crime Dot Com. In this book, investigative journalist Geoff White charts the astonishing development of hacking, from its conception in the United States' hippy tech community in the 1970s, through its childhood among the ruins of the Eastern Bloc, to its coming of age as one of the most dangerous and pervasive threats to our connected world. He takes us inside the workings of real-life cybercrimes, drawing on interviews with those behind the most devastating hacks and revealing how the tactics employed by high-tech crooks to make millions are being harnessed by nation states to target voters, cripple power networks, and even prepare for cyber-war. From Anonymous to the Dark Web, Ashley Madison to election rigging, Crime Dot Com is a thrilling, dizzying, and terrifying account of hacking, past and present, what the future has in store, and how we might protect ourselves from it.

NEW YORK TIMES BESTSELLER The complete, uncensored history of the award-winning The Daily Show with Jon Stewart, as told by its correspondents, writers, and host. For almost seventeen years, The Daily Show with Jon Stewart brilliantly redefined the borders between television comedy, political satire, and opinionated news coverage. It launched the careers of some of today's most significant comedians, highlighted the hypocrisies of the powerful, and garnered 23 Emmys. Now the show's behind-the-scenes gags, controversies, and camaraderie will be chronicled by the players themselves, from legendary host Jon Stewart to the star cast members and writers-including Samantha Bee, Stephen Colbert, John Oliver, and Steve Carell - plus some of The Daily Show's most prominent guests and adversaries: John and Cindy McCain, Glenn Beck, Tucker Carlson, and many more. This oral history takes the reader behind the curtain for all the show's highlights, from its origins as Comedy Central's underdog late-night program to Trevor Noah's succession, rising from a scrappy jester in the 24-hour political news cycle to become part of the beating heart of politics-a trusted source for not only comedy but also commentary, with a reputation for calling bullshit and an ability to effect real change in the world. Through years of incisive election coverage, passionate debates with President Obama and Hillary Clinton, feuds with Bill O'Reilly and Fox, and provocative takes on Wall Street and racism, The Daily Show has been a cultural touchstone. Now, for the first time, the people behind the show's seminal moments come together to share their memories of the last-minute rewrites, improvisations, pranks, romances, blow-ups, and moments of Zen both on and off the set of one of America's most groundbreaking shows.

Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It

An Introduction to Solving Crimes in Cyberspace

Nation

The Daily Show (The Book)

Stuxnet and the Launch of the World's First Digital Weapon

Inside the Business of Cybercrime

Fight Fire with Fire

Dawn of the Code War

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.

Building an Effective Security Program provides readers with a comprehensive approach to securing the IT systems in use at their organizations. This book provides information on how to structure and operate an effective cybersecurity program that includes people, processes, technologies, security awareness, and training. This program will establish and maintain effective security protections for the confidentiality, availability, and integrity of organization information. In this book, the authors take a pragmatic approach to building organization cyberdefenses that are effective while also remaining affordable. This book is intended for business leaders, IT professionals, cybersecurity personnel, educators, and students interested in deploying real-world cyberdefenses against today's persistent and sometimes devastating cyberattacks. It includes detailed explanation of the following IT security topics: IT Security Mindset—Think like an IT security professional, and consider how your IT environment can be defended against potential cyberattacks. Risk Management—Identify the assets, vulnerabilities and threats that drive IT risk, along with the controls that can be used to mitigate such risk. Effective Cyberdefense—Consider the components of an effective organization cyberdefense to successfully protect computers, devices, networks, accounts, applications and data. Cyber Operations—Operate cyberdefense capabilities and controls so that assets are protected, and intruders can be detected and repelled before significant damage can be done. IT Security Awareness and Training—Promote effective cybersecurity practices at work, on travel, and at home, among your organization's business leaders, IT professionals, and staff. Resilient IT Security—Implement, operate, monitor, assess, and improve your cybersecurity program on an ongoing basis to defend against the cyber threats of today and the future.

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 inside story of how America's enemies launched a cyber war against us-and how we've learned to fight back With each passing year, the internet-linked attacks on America's interests have grown in both frequency and severity. Overmatched by our military, countries like North Korea, China, Iran, and Russia have found us vulnerable in cyberspace. The "Code War" is upon us. In this dramatic book, former Assistant Attorney General John P. Carlin takes readers to the front lines of a global but little-understood fight as the Justice Department and the FBI chases down hackers, online terrorist recruiters, and spies. Today, as our entire economy goes digital, from banking to manufacturing to transportation, the potential targets for our enemies multiply. This firsthand account is both a remarkable untold story and a warning of dangers yet to come.