Hackers Heroes Of The Computer Revolution 25th Anniversary Edition

The Newsweek technology writer chronicles the rise of the Mac, a machine that revolutionized the computer industry and American society. Original.

Easy to understand and fun to read, this updated edition of Introducing Python is ideal for beginning programmers as well as those new to the language. Author Bill Lubanovic takes you from the basics to more involved and varied topics, mixing tutorials with cookbook-style code recipes to explain concepts in Python 3. End-of-chapter exercises help you practice what you've learned. You'll gain a strong foundation in the language, including best practices for testing, debugging, code reuse, and other development tips. This book also shows you how to use Python for applications in business, science, and the arts, using various Python tools and open source packages.

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.

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.

"The most interesting book ever written about Google" (The Washington Post) delivers the inside story behind the most successful and admired technology company of our time, now updated with a new Afterword. Google is arguably the most important company in the world today, with such pervasive influence that its name is a verb. The company founded by two Stanford graduate students—Larry Page and Sergey Brin—has become a tech giant known the world over. Since starting with its search engine, Google has moved into mobile phones, computer operating systems, power utilities, self-driving cars, all while remaining the most powerful company in the advertising business. Granted unprecedented access to the company, Levy disclosed that the key to Google's success in all these businesses lay in its engineering mindset and adoption of certain internet values such as speed, openness, experimentation, and risk-taking. Levy discloses details behind Google's relationship with China, including how Brin disagreed with his colleagues on the China strategy—and why its social networking initiative failed; the first time Google tried chasing a successful competitor. He examines Google's rocky relationship with government regulators, particularly in the EU, and how it has responded when employees left the company for smaller, nimbler start-ups. In the Plex is the "most authoritative…and in many ways the most entertaining" (James Gleick, The New York Book Review) account of Google to date and offers "an instructive primer on how the minds behind the world's most influential internet company function" (Richard Waters, The Wall Street Journal).

A noted journalist chronicles three years in the lives of a team of maverick software developers, led by Lotus 1-2-3 creator Mitch Kapor, intent on creating a revolutionary personal information manager to challenge Microsoft Outlook. Reprint. 30,000 first printing.

Hackers as vital disruptors, inspiring a new wave of activism in which ordinary citizens take back democracy. Hackers have a bad reputation, as shady deployers of bots and destroyers of infrastructure. In Coding Democracy, Maureen Webb offers another view. Hackers, she argues, can be vital disruptors. Hacking is becoming a practice, an ethos, and a metaphor for a new wave of activism in which ordinary citizens are inventing new forms of distributed, decentralized democracy for a digital era. Confronted with concentrations of power, mass surveillance, and authoritarianism enabled by new technology, the hacking movement is trying to "build out" democracy into cyberspace.

The author argues that we have reached the nadir of the adaptive range of our industrialised world. Now faced with an unsustainable trilemma of social, organisational and economic complexity, we have entered an era in which the rules we have previously organised our lives around no longer apply. Leaving us with both a design problem and a design challenge which we must urgently solve. By describing an entirely new way for true social, economic and organisational innovation to happen, No straight lines presents a revolutionary logic and an inspiring plea for a more human-centric world.

One of the Best Technology Books of 2020—Financial Times “Levy’s all-access Facebook reflects the reputational swan dive of its subject. . . . The result is evenhanded and devastating.”—San Francisco Chronicle “[Levy’s] evenhanded conclusions are still damning.”—Reason “[He] doesn’t shy from asking the tough questions.”—The Washington Post “Reminds you the HBO show Silicon Valley did not have to reach far for its satire.”—NPR.org The definitive history, packed with untold stories, of one of America’s most controversial and powerful companies: Facebook As a college sophomore, Mark Zuckerberg created a simple website to serve as a campus social network. Today, Facebook is nearly unrecognizable from its first, modest iteration. In light of recent controversies surrounding election-influencing “fake news” accounts, the handling of its users’ personal data, and growing discontent with the actions of its founder and CEO—who has enormous power over what the world sees and says—never has a company been more central to the national conversation. Millions of words have been written about Facebook, but no one has told the complete story, documenting its ascendancy and missteps. There is no denying the power and omnipresence of Facebook in American daily life, or the imperative of this book to document the unchecked power and shocking techniques of the company, from growing at all costs to outmaneuvering its biggest rivals to acquire WhatsApp and Instagram, to developing a platform so addictive even some of its own are now beginning to realize its dangers. Based on hundreds of interviews from inside and outside Facebook, Levy’s sweeping narrative of incredible entrepreneurial success and failure digs deep into the whole story of the company that has changed the world and reaped the consequences.

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

The bestselling cyberpunk author “has produced by far the most stylish report from the computer outlaw culture since Steven Levy’s Hackers” (Publishers Weekly). Bruce Sterling delves into the world of high-tech crime and punishment in one of the first books to explore the cyberspace breaches that threaten national security. From the crash of AT&T’s long-distance switching system to corporate cyberattacks, he investigates government and law enforcement efforts to break the back of America’s electronic underground in the 1990s. In this modern classic, “Sterling makes the hackers—who live in the ether between terminals under noms de net such as VaxCat—as vivid as Wyatt Earp and Doc Holliday. His book goes a long way towards explaining the emerging digital world and its ethos” (Publishers Weekly). This edition features a new preface by the author that analyzes the sobering increase in computer crime over the twenty-five years since The Hacker Crackdown was first published. “Offbeat and brilliant.” —Booklist “Thoroughly researched, this account of the government’s crackdown on the nebulous but growing computer-underground provides a thoughtful report on the laws and rights being defined on the virtual frontier of cyberspace. . . . An enjoyable, informative, and (as the first mainstream treatment of the subject) potentially important book . . . Sterling is a fine and knowledgeable guide to this strange new world.” —Kirkus Reviews “A well-balanced look at this new group of civil libertarians. Written with humor and intelligence, this book is highly recommended.” —Library Journal

Twenty five years ago, it didn't exist. Today, twenty million people worldwide are surfing the Net. Where Wizards Stay Up Late is the exciting story of the pioneers responsible for creating the most talked about, most influential, and most far-reaching communications breakthrough since the invention of the telephone. In the 1960's, when computers where regarded as mere giant calculators, J.C.R. Licklider at MIT saw them as the ultimate communications devices. With Defense Department funds, he and a band of visionary computer whizzes began work on a nationwide, interlocking network of computers. Taking readers behind the scenes, Where Wizards Stay Up Late captures the hard work, genius, and happy accidents of their daring, stunningly successful venture.

Suelette Dreyfus and her co-author, WikiLeaks founder Julian Assange, tell the extraordinary true story of the computer underground, and the bizarre lives and crimes of an elite ring of international hackers who took on the establishment. Spanning three continents and a decade of high level infiltration, they created chaos amongst some of the world's biggest and most powerful organisations, including NASA and the US military. Brilliant and obsessed, many of them found themselves addicted to hacking and phreaking. Some descended into drugs and madness, others ended up in jail. As riveting as the finest detective novel and meticulously researched, Underground follows the hackers through their crimes, their betrayals, the hunt, raids and investigations. It is a gripping tale of the digital underground.

Presents instructions for creating Android applications for mobile devices using Java.

With groundbreaking profiles of computer pioneers such as Bill Gates, Steve Wozinak, MIT's Tech Model Railroad Club, and more, "Hackers" captures a seminal moment with risk-takers and explorers who were poised to conquer 20th century America's last great frontier.

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

HackersHeroes of the Computer Revolution - 25th Anniversary Edition"O'Reilly Media, Inc."

This 25th anniversary edition of Steven Levy's classic book traces the exploits of the computer revolution's original hackers -- those brilliant and eccentric nerds from the late 1950s through the early '80s who took risks, bent the rules, and pushed the world in a radical new direction. With updated material from noteworthy hackers such as Bill Gates, Mark Zuckerberg, Richard Stallman, and Steve Wozniak, Hackers is a fascinating story that begins in early computer research labs and leads to the first home computers. Levy profiles the imaginative brainiacs who found clever and unorthodox solutions to computer engineering problems. They had a shared sense of values, known as "the hacker ethic," that still thrives today. Hackers captures a seminal period in recent history when underground activities blazed a trail for today's digital world, from MIT students finagling access to clunky computer-card machines to the DIY culture that spawned the Altair and the Apple II.

Prepare for the new Certified Ethical Hacker version 8 exam with this Sybex guide Security professionals remain in high demand. The Certified Ethical Hacker is a one-of-a-kind certification designed to give the candidate a look inside the mind of a hacker. This study guide provides a concise, easy-to-follow approach that covers all of the exam objectives and includes numerous examples and hands-on exercises. Coverage includes cryptography, footprinting and reconnaissance, scanning networks, enumeration of services, gaining access to a system, Trojans, viruses, worms, covert channels, and much more. A companion website includes additional study tools, Including practice exam and chapter review questions and electronic flashcards. Security remains the fastest growing segment of IT, and CEH certification provides unique skills The CEH also satisfies the Department of Defense’s 8570 Directive, which requires all Information Assurance government positions to hold one of the approved certifications This Sybex study guide is perfect for candidates studying on their own as well as those who are taking the CEHv8 course Covers all the exam objectives with an easy-to-follow approach Companion website includes practice exam questions, flashcards, and a searchable Glossary of key terms CEHv8: Certified Ethical Hacker Version 8 Study Guide is the book you need

when you're ready to tackle this challenging exam Also available as a set, Ethical Hacking and Web Hacking Set, 9781119072171 with The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition.

Cyber Wars gives you the dramatic inside stories of some of the world's biggest cyber attacks. These are the game changing hacks that make organizations around the world tremble and leaders stop and consider just how safe they really are. Charles Arthur provides a gripping account of why each hack happened, what techniques were used, what the consequences were and how they could have been prevented. Cyber attacks are some of the most frightening threats currently facing business leaders and this book provides a deep insight into understanding how they work, how hackers think as well as giving invaluable advice on staying vigilant and avoiding the security mistakes and oversights that can lead to downfall. No organization is safe but by understanding the context within which we now live and what the hacks of the future might look like, you can minimize the threat. In Cyber Wars, you will learn how hackers in a TK Maxx parking lot managed to steal 94m credit card details costing the organization $1bn; how a 17 year old leaked the data of 157,000 TalkTalk customers causing a reputational disaster; how Mirai can infect companies' Internet of Things devices and let hackers control them; how a sophisticated malware attack on Sony caused corporate embarrassment and company-wide shut down; and how a phishing attack on Clinton Campaign Chairman John Podesta's email affected the outcome of the 2016 US election.

This is "the Word" -- one man's word, certainly -- about the art (and artifice) of the state of our computer-centric existence. And considering that the "one man" is Neal Stephenson, "the hacker Hemingway" (Newsweek) -- acclaimed novelist, pragmatist, seer, nerd-friendly philosopher, and nationally bestselling author of groundbreaking literary works (Snow Crash, Cryptonomicon, etc., etc.) -- the word is well worth hearing. Mostly well-reasoned examination and partial rant, Stephenson's In the Beginning... was the Command Line is a thoughtful, irreverent, hilarious treatise on the cyber-culture past and present; on operating system tyrannies and downloaded popular revolutions; on the Internet, Disney World, Big Bangs, not to mention the meaning of life itself.

"This is the most important book on Silicon Valley I've read in two decades. It will take us all back to our roots in the counterculture, and will remind us of the true nature of the innovation process, before we tried to tame it with slogans and buzzwords." -- Po Bronson, #1 New York Times bestselling author of The Nudist on the Late Shift and Nurtureshock A candid, colorful, and comprehensive oral history that reveals the secrets of Silicon Valley -- from the origins of Apple and Atari to the present day clashes of Google and Facebook, and all the start-ups and disruptions that happened along the way. Rarely has one economy asserted itself as swiftly--and as aggressively--as the entity we now know as Silicon Valley. Built with a seemingly permanent culture of reinvention, Silicon Valley does not fight change; it embraces it, and now powers the American economy and global innovation. So how did this omnipotent and ever-morphing place come to be? It was not by planning. It was, like many an empire before it, part luck, part timing, and part ambition. And part pure, unbridled genius... Drawing on over two hundred in-depth interviews, Valley of Genius takes readers from the dawn of the personal computer and the internet, through the heyday of the web, up to the very moment when our current technological reality was invented. It interweaves accounts of invention and betrayal, overnight success and underground exploits, to tell the story of Silicon Valley like it has never been told before. Read it to discover the stories that Valley insiders tell each other: the tall tales that are all, improbably, true.

“One of the finest books on information security published so far in this century—easily accessible, tightly argued, superbly well-sourced, intimidatingly perceptive.” —Thomas Rid, author of Active Measures “The best examination I have read of how increasingly dramatic developments in cyberspace are defining the ‘new normal’ of geopolitics in the digital age. Buchanan...captures the dynamics of all of this truly brilliantly.” —General David Petraeus, former Director of the CIA and Commander of Coalition Forces in Iraq and Afghanistan Few national-security threats are as potent—or as nebulous—as cyber attacks. Ben Buchanan reveals how hackers are transforming spycraft and statecraft, catching us all in the crossfire, whether we know it or not. Ever since WarGames, we have been bracing for the cyberwar to come, conjuring images of exploding power plants and mass panic. But while cyber attacks are now disturbingly common, they don’t look anything like we thought they would. Packed with insider information based on interviews, declassified files, and forensic analysis of company reports, The Hacker and the State sets aside fantasies of cyber-annihilation to explore the real geopolitical competition of the digital age. Tracing the conflict of wills and interests among modern nations, Ben Buchanan reveals little-known details of how China, Russia, North Korea, Britain, and the United States hack one another in a relentless struggle for dominance. His analysis moves deftly from underseas cable taps to underground nuclear sabotage, from blackouts and data breaches to billion-dollar heists and election interference. Buchanan brings to life this continuous cycle of espionage and deception, attack and counterattack, destabilization and retaliation. He explains why cyber attacks are far less destructive than we anticipated, far more pervasive, and much harder to prevent. With little fanfare and far less scrutiny, they impact our banks, our tech and health systems, our democracy, and every aspect of our lives. Quietly, insidiously, they have reshaped our national-security priorities and transformed spycraft and statecraft. The contest for geopolitical advantage has moved into cyberspace. The United States and its allies can no longer dominate the way they once did. The nation that hacks best will triumph.

Provides step-by-step instructions for entering supposedly secure computer systems, along with a summary of the laws covering this generally illegal activity and an explanation of the role of hackers in maintaining computer security

The author examines issues such as the rightness of web-based applications, the programming language renaissance, spam filtering, the Open Source Movement, Internet startups and more.

He also tells important stories about the kinds of people behind technical innovations, revealing their character and their craft.
This book looks at artificial life science - A-Life, an important new area of scientific research involving the disciplines of microbiology, evolutionary theory, physics, chemistry and computer science. In the 1940s a mathematician named John von Neumann, a man with a claim to being the father of the modern computer, invented a hypothetical mathematical entity called a cellular automaton. His aim was to construct a machine that could reproduce itself. In the years since, with the development of hugely more sophisticated and complex computers, von Neumann's insights have gradually led to a point where scientists have created, within the wiring of these machines, something that so closely simulates life that it may, arguably, be called life. This machine reproduces itself, mutates, evolves through generations and dies.
The shocking untold story of the elite secret society of hackers fighting to protect our privacy, our freedom -- even democracy itself Cult of the Dead Cow is the tale of the oldest, most respected, and most famous American hacking group of all time. Though until now it has remained mostly anonymous, its members invented the concept of hacktivism, released the top tool for testing password security, and created what was for years the best technique for controlling computers from afar, forcing giant companies to work harder to protect customers. They contributed to the development of Tor, the most important privacy tool on the net, and helped build cyberweapons that advanced US security without injuring anyone. With its origins in the earliest days of the Internet, the cDc is full of oddball characters -- activists, artists, even future politicians. Many of these hackers have become top executives and advisors walking the corridors of power in Washington and Silicon Valley. The most famous is former Texas Congressman and current presidential candidate Beto O'Rourke, whose time in the cDc set him up to found a tech business, launch an alternative publication in El Paso, and make long-shot bets on unconventional campaigns. Today, the group and its followers are battling electoral misinformation, making personal data safer, and battling to keep technology a force for good instead of for surveillance and oppression. Cult of the Dead Cow shows how governments, corporations, and criminals came to hold immense power over individuals and how we can fight back against them.
"Extremely pleasurable... A gripping story with lots of good, meaty forbidden knowledge and insight into the hacker mindset." -- Cory Doctorow, Boing Boing "Wizzywig is a delight, wryly rendered and packed with dead-on details of the hacker life."-- Wired "Wizzywig is a portrait of a cultural moment when geeks weren't just outside mainstream culture but terrifying to it."-- TIME.com Techland They say What You See Is What You Get... but Kevin "Boingthump"Phenicle could always see more than most people. In the world of phone phreaks, hackers, and scammers, he's a legend. His exploits are hotly debated: could he really get free long-distance calls by whistling into a pay phone? Did his video-game piracy scheme accidentally trigger the first computer virus? And did he really dodge the FBI by using their own wiretapping software against them? Is he even a real person? And if he's ever caught, what would happen to a geek like him in federal prison? Inspired by the incredible stories of real-life hackers, WIZZYWIG is the thrilling tale of a master manipulator -- his journey from precocious child scammer to federally-wanted fugitive, and beyond. In a world transformed by social networks, data leaks, and digital uprisings, Ed Piskor's debut graphic novel reminds us how much power can rest in the hands of an audacious kid with a keyboard. -- A 288-page hardcover graphic novel, 6.5” x 9”. Ed's DIY releases of chapters of WIZZYWIG have already garnered substantial accolades and a cult fan base, and we are eager to share this book with the world.
You may be a hacker and not even know it. Being a hacker has nothing to do with cyberterrorism, and it doesn’t even necessarily relate to the open-source movement. Being a hacker has more to do with your underlying assumptions about stress, time management, work, and play. It’s about harmonizing the rhythms of your creative work with the rhythms of the rest of your life so that they amplify each other. It is a fundamentally new work ethic that is revolutionizing the way business is being done around the world. Without hackers there would be no universal access to e-mail, no Internet, no World Wide Web, but the hacker ethic has spread far beyond the world of computers. It is a mind-set, a philosophy, based on the values of play, passion, sharing, and creativity, that has the potential to enhance every individual’s and company’s productivity and competitiveness. Now there is a greater need than ever for entrepreneurial versatility of the sort that has made hackers the most important innovators of our day. Pekka Himanen shows how we all can make use of this ongoing transformation in the way we approach our working lives.
Most histories of the personal computer industry focus on technology or business. John Markoff’s landmark book is about the culture and consciousness behind the first PCs—the culture being counter– and the consciousness expanded, sometimes chemically. It’s a brilliant evocation of Stanford, California, in the 1960s and ’70s, where a group of visionaries set out to turn computers into a means for freeing minds and information. In these pages one encounters Ken Kesey and the phone hacker Cap’n Crunch, est and LSD, The Whole Earth Catalog and the Homebrew Computer Lab. What the Dormouse Said is a poignant, funny, and inspiring book by one of the smartest technology writers around.
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.
“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

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.

Hacking Europe traces the user practices of chopping games in Warsaw, hacking software in Athens, creating chaos in Hamburg, producing demos in Turku, and partying with computing in Zagreb and Amsterdam. Focusing on several European countries at the end of the Cold War, the book shows the digital development was not an exclusively American affair. Local hacker communities appropriated the computer and forged new cultures around it like the hackers in Yugoslavia, Poland and Finland, who showed off their tricks and creating distinct “demoscenes.” Together the essays reflect a diverse palette of cultural practices by which European users domesticated computer technologies. Each chapter explores the mediating actors instrumental in introducing and spreading the cultures of computing around Europe. More generally, the “ludological” element--the role of mischief, humor, and play--discussed here as crucial for analysis of hacker culture, opens new vistas for the study of the history of technology.

Let Over Lambda is one of the most hardcore computer programming books out there. Starting with the fundamentals, it describes the most advanced features of the most advanced language: Common Lisp. Only the top percentile of programmers use lisp and if you can understand this book you are in the top percentile of lisp programmers. If you are looking for a dry coding manual that re-hashes common-sense techniques in whatever langue du jour, this book is not for you. This book is about pushing the boundaries of what we know about programming. While this book teaches useful skills that can help solve your programming problems today and now, it has also been designed to be entertaining and inspiring. If you have ever wondered what lisp or even programming itself is really about, this is the book you have been looking for.

If you've ever made a secure purchase with your credit card over the Internet, then you have seen cryptography, or "crypto", in action. From Stephen Levy—the author who made "hackers" a household word—comes this account of a revolution that is already affecting every citizen in the twenty-first century. Crypto tells the inside story of how a group of "crypto rebels"—nerds and visionaries turned freedom fighters—teamed up with corporate interests to beat Big Brother and ensure our privacy on the Internet. Levy's history of one of the most controversial and important topics of the digital age reads like the best futuristic fiction.

The Metasploit Framework makes discovering, exploiting, and sharing vulnerabilities quick and relatively painless. But while Metasploit is used by security professionals everywhere, the tool can be hard to grasp for first-time users. Metasploit: The Penetration Tester's Guide fills this gap by teaching you how to harness the Framework and interact with the vibrant community of Metasploit contributors. Once you've built your foundation for penetration testing, you’ll learn the Framework's conventions, interfaces, and module system as you launch simulated attacks. You’ll move on to advanced penetration testing techniques, including network reconnaissance and enumeration, client-side attacks, wireless attacks, and targeted social-engineering attacks. Learn how to: –Find and exploit unmaintained, misconfigured, and unpatched systems –Perform reconnaissance and find valuable information about your target –Bypass anti-virus technologies and circumvent security controls –Integrate Nmap, NeXpose, and Nessus with Metasploit to automate discovery –Use the Meterpreter shell to launch further attacks from inside the network –Harness standalone Metasploit utilities, third-party tools, and plug-ins –Learn how to write your own Meterpreter post exploitation modules and scripts You'll even touch on exploit discovery for zero-day research, write a fuzzer, port existing exploits into the Framework, and learn how to cover your tracks. Whether your goal is to secure your own networks or to put someone else's to the test, Metasploit: The Penetration Tester's Guide will take you there and beyond.