2600 Magazine The Hacker Quarterly Winter 2016 2017

The definitive guide to hacking the world of the Internet of Things (IoT) -- Internet connected devices such as medical devices, home assistants, smart home appliances and more. Drawing from the real-life exploits of five highly regarded IoT security researchers, Practical IoT Hacking teaches you how to test IoT systems, devices, and protocols to mitigate risk. The book begins by walking you through common threats and a threat modeling framework. You'll develop a security testing methodology, discover the art of passive reconnaissance, and assess security on all layers of an IoT system. Next, you'll perform VLAN hopping, crack MQTT authentication, abuse UPnP, develop an mDNS poisoner, and craft WS-Discovery attacks. You'll tackle both hardware hacking and radio hacking, with in-depth coverage of attacks against embedded IoT devices and RFID systems. You'll also learn how to: • Write a DICOM service scanner as an NSE module • Hack a microcontroller through the UART and SWD interfaces • Reverse engineer firmware and analyze mobile companion apps • Develop an NFC fuzzer using Proxmark3 • Hack a smart home by jamming wireless alarms, playing back IP camera feeds, and controlling a smart treadmill The tools and devices you'll use are affordable and readily available, so you can easily practice what you learn. Whether you’re a security researcher, IT team member, or hacking hobbyist, you’ll find Practical IoT Hacking indispensable in your efforts to hack all the things REQUIREMENTS: Basic knowledge of Linux command line, TCP/IP, and programming

Osteoporosis is a preventable disease. With knowing the right foods to eat you can improve your overall bone strength and prevent osteoporosis. It is a popular notion that osteoporosis is unavoidable. Growing old affects bone health and whether we like it or not, bones will become weak and osteoporosis will set in sooner or later. This is not true because studies show that osteoporosis is preventable. A lifestyle that includes healthy eating, good habits and regular exercise can help prevent the disease. In this book, I will share how nutrition plays an important role when it comes to bone health. This book will teach you what types of food you should eat more of and what types of food you should avoid. I will lay it all out step by step. After reading this book you will see how simple it is to keep your bones strong and prevent osteoporosis. Twenty or thirty years from now you will be so glad you stumbled upon this book and read it. I wish you all the success in the world as you embark on the road to better health through the osteoporosis diet. You can improve your bone strength and prevent osteoporosis and this book will help you do it!

If you thought hacking was just about mischief-makers hunched over computers in the basement, think again. As seasoned author Wallace Wang explains, hacking can also mean questioning the status quo, looking for your own truths and never accepting at face value anything authorities say or do. The completely revised fourth edition of this offbeat, non-technical book examines what hackers do, how they do it, and how you can protect yourself. Written in the same informative, irreverent, and entertaining style that made the first three editions hugely successful, Steal This Computer Book 4.0 will expand your mind and raise your eyebrows. New chapters discuss the hacker mentality, social engineering and lock picking, exploiting P2P file-sharing networks, and how people manipulate search engines and pop-up ads to obtain and use personal information. Wang also takes issue with the media for "hacking" the news and presenting the public with self-serving stories of questionable accuracy. Inside, you’ll discover: –How to manage and fight spam and spyware –How Trojan horse programs and rootkits work and how to defend against them –How hackers steal software and defeat copy-protection mechanisms –How to tell if your machine is being attacked and what you can do to protect it –Where the hackers are, how they probe a target and sneak into a computer, and what they do once they get inside –How corporations use hacker techniques to infect your computer and invade your privacy –How you can lock down your computer to protect your data and your personal information using free programs included on the book's CD If you've ever logged onto a website, conducted an online transaction, sent or received email, used a networked computer or even watched the evening news, you may have already been tricked, tracked, hacked, and manipulated. As the saying goes, just because you're paranoid doesn't mean they aren't after you. And, as Wallace Wang reveals, they probably are. The companion CD contains hundreds of megabytes of 100% FREE hacking and security related programs, like keyloggers, spyware stoppers, port blockers, IP scanners, Trojan horse detectors, and much, much more. CD compatible with Windows, Mac, and Linux.

The million-copy New York Times bestseller from the Fox News anchor who's brought new excitement–and massive amounts of populist common sense and rock-solid honesty–to television news. Now four seasons strong, Bill O'Reilly's nightly cable news program, "The O'Reilly Factor," is one of the hottest shows on the air. In book form, The O'Reilly Factor has sold over a million copies and spent fourteen weeks at the top of the New York Times bestseller list. Obviously, Bill O'Reilly has made his mark. His blunt, ironic, no-holds-barred style has earned him a devoted audience–friends and foes alike–who send him five thousand letters every week. And with the wit and intelligence that have made him one of the most talked-about stars in both television and publishing, O'Reilly continues to identify what's right, what's wrong, and what's absurd in the political, social, economic, and cultural life of America.

As an open operating system, Unix can be improved on by anyone and everyone: individuals, companies, universities, and more. As a result, the very nature of Unix has been altered over the years by numerous extensions formulated in an assortment of versions. Today, Unix encompasses everything from Sun's Solaris to Apple's Mac OS X and more varieties of Linux than you can easily name. The latest edition of this bestselling reference brings Unix into the 21st century. It's been reworked to keep current with the broader state of Unix in today's world and highlight the strengths of this operating system in all its various flavors. Detailing all Unix commands and options, the informative guide provides generous descriptions and examples that put those commands in context. Here are some of the new features you'll find in Unix in a Nutshell, Fourth Edition: Solaris 10, the latest version of the SVR4-based operating system, GNU/Linux, and Mac OS X Bash shell (along with the 1988 and 1993 versions of ksh) tsch shell (instead of the original Berkeley csh) Package management programs, used for program installation on popular GNU/Linux systems, Solaris and Mac OS X

GNU Emacs Version 21 Introduction to source code management systems Concurrent versions system Subversion version control system GDB debugger As Unix has progressed, certain commands that were once critical have fallen into disuse. To that end, the book has also dropped material that is no longer relevant, keeping it taut and current. If you're a Unix user or programmer, you'll recognize the value of this complete, up-to-date Unix reference. With chapter overviews, specific examples, and detailed command.

When her research is being used to run unmanned drones, Lindsey McKinney and Odin, a Special Ops soldier with an insight into the faceless enemy, must slow the advance long enough for the world to recognize its destructive power.

The Hands-On, Practical Guide to Preventing Ajax-Related Security Vulnerabilities More and more Web sites are being rewritten as Ajax applications; even traditional desktop software is rapidly moving to the Web via Ajax. But, all too often, this transition is being made with reckless disregard for security. If Ajax applications aren’t designed and coded properly, they can be susceptible to far more dangerous security vulnerabilities than conventional Web or desktop software. Ajax developers desperately need guidance on securing their applications: knowledge that’s been virtually impossible to find, until now. Ajax Security systematically debunks today’s most dangerous myths about Ajax security, illustrating key points with detailed case studies of actual exploited Ajax vulnerabilities, ranging from MySpace’s Samy worm to MacWorld’s conference code validator. Even more important, it delivers specific, up-to-the-minute recommendations for securing Ajax applications in each major Web programming language and environment, including .NET, Java, PHP, and even Ruby on Rails. You’ll learn how to: · Mitigate unique risks associated with Ajax, including overly granular Web services, application control flow tampering, and manipulation of program logic · Write new Ajax code more safely—and identify and fix flaws in existing code · Prevent emerging Ajax-specific attacks, including JavaScript hijacking and persistent storage theft · Avoid attacks based on XSS and SQL Injection—including a dangerous SQL Injection variant that can extract an entire backend database with just two requests · Leverage security built into Ajax frameworks like Prototype, Dojo, and ASP.NET AJAX Extensions—and recognize what you still must implement on your own · Create more secure “mashup” applications Ajax Security will be an indispensable resource for developers coding or maintaining Ajax applications; architects and development managers planning or designing new Ajax software, and all software security professionals, from QA specialists to penetration testers.

Since 1984, the quarterly magazine 2600 has provided fascinating articles for readers who are curious about technology. Find the best of the magazine’s writing in Best of 2600: A Hacker Odyssey, a collection of the strongest, most interesting, and often most controversial articles covering 24 years of changes in technology, all from a hacker’s perspective. Included are stories about the creation of the infamous tone dialer “red box” that allowed hackers to make free phone calls from payphones, the founding of the Electronic Frontier Foundation, and the insecurity of modern locks.

Presents instructions for creating and enhancing a variety of projects, including a sandwich-making robot, a Twitter-monitoring Christmas tree, and a bronze-melting blast furnace.

Be smarter than your computer If you don't understand computers, you can quickly be left behind in today's fast-paced, machine-dependent society. Computer Science Made Simple offers a straightforward resource for technology novices and advanced techies alike. It clarifies all you need to know, from the basic components of today’s computers to using advanced applications. The perfect primer, it explains how it all comes together to make computers work. Topics covered include: * hardware * software * programming * networks * the internet * computer graphics * advanced computer concepts * computers in society Look for these Made Simple titles: Accounting Made Simple Arithmetic Made Simple Astronomy Made Simple Biology Made Simple Bookkeeping Made Simple Business Letters Made Simple Chemistry Made Simple Earth Science Made Simple English Made Simple French Made Simple German Made Simple Inglés Hecho Fácil Investing Made Simple Italian Made Simple Keyboarding Made Simple Latin Made Simple Learning English Made Simple Mathematics Made Simple

The Perfect Business Plan Made Simple Philosophy Made Simple Physics Made Simple Psychology Made Simple Sign Language Made Simple Spanish Made Simple Spelling Made Simple Statistics Made Simple Your Small Business Made Simple www.broadway.com

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 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

Voice over Internet Protocol is gaining a lot of attention these days. Both practical and fun, this text provides technology enthusiasts and voice professionals with dozens of hands-on projects for building a VoIP network, including a softPBX.

On Australia's hottest beach, the most dangerous current is between them. Training to be a lifeguard is tough work, but Cody Grant loves a challenge. He spends long days in the sun and surf rescuing swimmers from treacherous rip currents while trying not to lust after senior lifeguard Liam Fox-who is deeply, painfully closeted. Liam was supposed to be a football legend. Now in his mid-thirties, it's been over a decade since his dream shattered along with his knee. Fans still recognize him regularly, and he's terrified his sexuality will be discovered and his conservative parents will reject him. He has strict rules to protect his secret and keeps everyone at arm's length. Liam never acts on his need to surrender after being shamed for it years ago by the first and only man he trusted. Out and proud Cody fascinates Liam-and tempts him to break all the rules. Cody is practically half Liam's size and age, but has the confidence and compassion to take charge and give Liam the release, affection, and acceptance he desperately craves. But how long can a secret affair satisfy their hearts? As if saving lives isn't hard enough, Cody faces his greatest challenge yet convincing Liam to trust him and find the courage to live out loud. Flash Rip is an M/M gay romance from Keira Andrews featuring a slow burn, an age gap, scorching first times, and of course a happy ending.

One of America's most experienced agents offers a glimpse inside the shadowy world of counterrorism to reveal life on the frontlines of the war on terrorism, detailing his experiences with the Diplomatic Security Service in every area of the world.

London-based American journalist Grossman continues her coverage of the Internet by assessing the battles she believes will define its future. Among them are scams, class divisions, privacy, the Communications Decency Act, women online, pornography, hackers and the computer underground, criminals, and sociopaths. Annotation copyrighted by Book News, Inc., Portland, OR

Defines over eight hundred terms, including legal cases and people, related to computer hacking and computer security; provides a chronology of events related to hacking; and describes the ways in which hackers work.

"Physicist Jon Grady and his team have discovered a device that can reflect gravity. But instead of Grady getting acclaim, his lab is locked down by a covert organization known as the Bureau of Technology Control. When Grady refuses to join the BTC, he's thrown into a nightmarish high-tech prison. Now Grady and his fellow prisoners must try to expose the secrets of an unimaginable enemy"--Back cover.

Daniel Suarez’s New York Times bestselling debut high-tech thriller is “so frightening even the government has taken note” (Entertainment Weekly). Daemons: computer programs that silently run in the background, waiting for a specific event or time to execute. They power almost every service. They make our networked world possible. But they also make it vulnerable... When the obituary of legendary computer game architect Matthew Sobol appears online, a previously dormant daemon activates, initiating a chain of events that begins to unravel our interconnected world. This daemon reads news headlines, recruits human followers, and orders assassinations. With Sobol’s secrets buried with him, and as new layers of his daemon are unleashed, it’s up to Detective Peter Sebeck to stop a self-replicating virtual killer before it achieves its ultimate purpose—one that goes far beyond anything Sebeck could have imagined...

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.

This riveting work of investigative reporting and history exposes classified government projects to build gravity-defying aircraft--which have an uncanny resemblance to flying saucers. The atomic bomb was not the only project to occupy government scientists in the 1940s. Antigravity technology, originally spearheaded by scientists in Nazi Germany, was another high priority, one that still may be in effect today. Now for the first time, a reporter with an unprecedented access to key sources in the intelligence and military communities reveals suppressed evidence that tells the story of a quest for a discovery that could prove as powerful as the A-bomb. The Hunt for Zero Point explores the scientific speculation that a "zero point" of gravity exists in the universe and can be replicated here on Earth. The pressure to be the first nation to harness gravity is immense, as it means having the ability to build military planes of unlimited speed and range, along with the most deadly weaponry the world has ever seen. The ideal shape for a gravity-defying vehicle happens to be a perfect disk, making antigravity tests a possible explanation for the numerous UFO sightings of the past 50 years. Chronicling the origins of antigravity research in the world's most advanced research facility, which was operated by the Third Reich during World War II, The Hunt for Zero Point traces U.S. involvement in the project, beginning with the recruitment of former Nazi scientists after the war. Drawn from interviews with those involved with the research and who visited labs in Europe and the United States, The Hunt for Zero Point journeys to the heart of the twentieth century's most puzzling unexplained phenomena.

A thrilling, exclusive expose of the hacker collectives Anonymous and LulzSec. WE ARE ANONYMOUS is the first full account of how a loosely assembled group of hackers scattered across the globe formed a new kind of insurgency, seized headlines, and tortured the feds-and the ultimate betrayal that would eventually bring them down. Parmy Olson goes behind the headlines and into the world of Anonymous and LulzSec with unprecedented access, drawing upon hundreds of conversations with the hackers themselves, including exclusive interviews with all six core members of LulzSec. In late 2010, thousands of hacktivists joined a mass digital assault on the websites of VISA, MasterCard, and PayPal to protest their treatment of WikiLeaks. Other targets were wide ranging-the websites of corporations from Sony Entertainment and Fox to the Vatican and the Church of Scientology were hacked, defaced, and embarrassed-and the message was that no one was safe. Thousands of user accounts from pornography websites were released, exposing government employees and military personnel. Although some attacks were perpetrated by masses of users who were rallied on the message boards of 4Chan, many others were masterminded by a small, tight-knit group of hackers who formed a splinter group of Anonymous called LulzSec. The legend of Anonymous and LulzSec grew in the wake of each ambitious hack. But how were they penetrating intricate corporate security systems? Were they anarchists or activists? Teams or lone wolves? A cabal of skilled hackers or a disorganized bunch of kids? WE ARE ANONYMOUS delves deep into the internet's underbelly to tell the incredible full story of the global cyber insurgency movement, and its implications for the future of computer security.

Who are computer hackers? What is free software? And what does the emergence of a community dedicated to the production of free and open source software--and to hacking as a technical, aesthetic, and moral project--reveal about the values of contemporary liberalism? Exploring the rise and political significance of the free and open source software (F/OSS) movement in the United States and Europe, Coding Freedom details the ethics behind hackers' devotion to F/OSS, the social codes that guide its production, and the political struggles through which hackers question the scope and direction of copyright and patent law. In telling the story of the F/OSS movement, the book unfolds a broader narrative involving computing, the politics of access, and intellectual property. E. Gabriella Coleman tracks the ways in which hackers collaborate and examines passionate manifestos, hacker humor, free software project governance, and festive hacker conferences. Looking at the ways that hackers sustain their productive freedom, Coleman shows that these activists, driven by a commitment to their work, reformulate key ideals including free speech, transparency, and meritocracy, and refuse restrictive intellectual protections. Coleman demonstrates how hacking, so often marginalized or misunderstood, sheds light on the continuing relevance of liberalism in online collaboration.

Cybersecurity jobs confines from basic configuration to advanced systems analysis and defense assessment. Cybersecurity: The Beginner's Guide provides thefundamental information you need to understand the basics of the field, identify your place within it, and start your Cybersecurity career.

A fast, hands-on introduction to offensive hacking techniques Hands-On Hacking teaches readers to see through the eyes of their adversary and apply hacking techniques to better understand real-world risks to computer networks and data. Readers will benefit from the author's years of experience in the field hacking into computer networks and ultimately training others in the art of cyber-attacks. This book holds no punches and explains the tools, tactics and procedures used by ethical hackers and criminal crackers alike. We will take you on a journey through a hacker’s perspective when focused on the computer infrastructure of a target company, exploring how to access the servers and data. Once the information gathering stage is complete, you’ll look for flaws and their known exploits—including tools developed by real-world government financed state-actors. • An introduction to the same hacking techniques that malicious hackers will use against an organization • Written by infosec experts with proven history of publishing vulnerabilities and highlighting security flaws • Based on the tried and tested material used to train hackers all over the world in the art of breaching networks • Covers the fundamental basics of how computer networks are inherently vulnerable to attack, teaching the student how to apply hacking skills to uncover vulnerabilities We cover topics of breaching a company from the external network perimeter, hacking internal enterprise systems and web application vulnerabilities. Delving into the basics of exploitation with real-world practical examples, you won’t find any hypothetical academic only attacks here. From start to finish this book will take the student through the steps necessary to breach an organization to improve its security. Written by world-renowned cybersecurity experts and educators, Hands-On Hacking teaches entry-level professionals seeking to learn ethical hacking techniques. If you are looking to understand penetration testing and ethical hacking, this book takes you from basic methods to advanced techniques in a structured learning format.

Dario may not have his life figured out, but at least he has a job, a cell phone, and friends who care about him. That's enough, until the circus comes to town. Soon after, a bloody attack puts his friend in the hospital and Dario begins to hunt for whoever is responsible. As he investigates, Dario is pulled toward the dangerous and violent circus, its strange people, and the dark rumors of "Frank's Show". But the more he unravels the mystery, the more he realizes he must escape it all... before it kills him.

Become a cyber-hero - know the common wireless weaknesses "Reading a book like this one is a worthy endeavor towardbecoming an experienced wireless security professional." --Devin Akin - CTO, The Certified Wireless Network Professional(CWNP) Program Wireless networks are so convenient - not only for you, but alsofor those nefarious types who'd like to invade them. The only wayto know if your system can be penetrated is to simulate an attack.This book shows you how, along with how to strengthen any weakspots you find in your network's armor. Discover how to: Perform ethical hacks without compromising a system Combat denial of service and WEP attacks Understand how invaders think Recognize the effects of different hacks Protect against war drivers and rogue devices

The authors take readers on a story-packed adventure through the history of LEGO, from its

humble beginnings in a small Danish village to its ascent to the summit of the toy world. They learn hundreds of obscure LEGO facts as they're surrounded by countless fantastically complex and challenging models built by some of the most famous adult LEGO builders.
Ghost in the WiresMy Adventures as the World's Most Wanted HackerLittle, Brown
Fully-updated for Python 3, the second edition of this worldwide bestseller (over 100,000 copies sold) explores the stealthier side of programming and brings you all new strategies for your hacking projects. When it comes to creating powerful and effective hacking tools, Python is the language of choice for most security analysts. In Black Hat Python, 2nd Edition, you’ll explore the darker side of Python’s capabilities—writing network sniffers, stealing email credentials, brute forcing directories, crafting mutation fuzzers, infecting virtual machines, creating stealthy trojans, and more. The second edition of this bestselling hacking book contains code updated for the latest version of Python 3, as well as new techniques that reflect current industry best practices. You’ll also find expanded explanations of Python libraries such as ctypes, struct, lxml, and BeautifulSoup, and dig deeper into strategies, from splitting bytes to leveraging computer-vision libraries, that you can apply to future hacking projects. You’ll learn how to: • Create a trojan command-and-control using GitHub • Detect sandboxing and automate common malware tasks, like keylogging and screenshotting • Escalate Windows privileges with creative process control • Use offensive memory forensics tricks to retrieve password hashes and inject shellcode into a virtual machine • Extend the popular Burp Suite web-hacking tool • Abuse Windows COM automation to perform a man-in-the-browser attack • Exfiltrate data from a network most sneakily When it comes to offensive security, your ability to create powerful tools on the fly is indispensable. Learn how with the second edition of Black

Hat Python. New to this edition: All Python code has been updated to cover Python 3 and includes updated libraries used in current Python applications. Additionally, there are more in-depth explanations of the code and the programming techniques have been updated to current, common tactics. Examples of new material that you'll learn include how to sniff network traffic, evade anti-virus software, brute-force web applications, and set up a command-and-control (C2) system using GitHub.

2045. Kenneth Durand leads Interpol's most effective team against genetic crime, hunting down black market labs that perform illegal procedures, augmenting embryos and rapidly accelerating human evolution-- and preying on human-trafficking victims to experiment and advance their technology. One figure looms behind it all: Marcus Demang Wyckes, leader of a cartel known as the Huli jing. When Durand is forcibly dosed with a radical new change agent, he wakes from a coma weeks later to find he's been genetically transformed into Wyckes. Determined to restore his original DNA, Durand hasn't anticipated just how difficult locating his enemy will be.

“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

Way back in the last century, back in the 1960s, computers were mammoth mysterious machines. They were immensely expensive yet became essential to daily business operations. Yet, no one ever saw them. Security dictated they be hidden away. Only the computer operators were allowed access. These were the important people who actually made the computer do useful work. On the other hand, these knowledgeable operators knew absolutely nothing of the technology behind the covers. Whenever a problem arose, there was no choice but to call the Computer Guy. Frantically a supervisor would place a call for service. Then wait. And wait. Little could be done without the computer running. Finally! At long last, someone would yell out, "The computer guy is here!" Following a brief greeting, the thankful supervisor immediately wanted to know how long it would take to get the computer running again. So, with everyone anxiously looking over his shoulder, the computer guy set about his business of determining the cause and finding a solution to the problem. Clearly a stressful situation. Yet this was only a minor portion of an essential career from the early days of the Computer Era. The Computer Guys were the Field Engineers who installed, maintained and repaired those old mainframe computers. Their place in technological history is finally documented.

Social media ... perhaps the most pointless waste of time since the invention of the television. Yet unlike television, you don't just have to sit back and be on the receiving end of useless information and opinions. No, you can broadcast your own banality!Here is a book of the sort of tosh that social media fills our lives with (if we let it) ... and yet ... there is the occasional wise or useful snippet that almost makes you think social media could have some sort of useful contribution to make to life ... if only we could cut out 99% of the 'twats' and 99% of the 'twits' they send out!

Presents instructions for creating and enhancing a variety of household electronic equipment, including a magnetic stripe card reader, a video camera stabilizer, and a glowstick.

The Anarchist Cookbook will shock, it will disturb, it will provoke. It places in historical perspective an era when "Turn on, Burn down, Blow up" are revolutionary slogans of the day. Says the author" "This book... is not written for the members of fringe political groups, such as the Weatherman, or The Minutemen. Those radical groups don't need this book. They already know everything that's in here. If the real people of America, the silent majority, are going to survive, they must educate themselves. That is the purpose of this book." In what the author considers a survival guide, there is explicit information on the uses and effects of drugs, ranging from pot to heroin to peanuts. There i detailed advice concerning electronics, sabotage, and surveillance, with data on everything from bugs to scramblers. There is a comprehensive chapter on natural, non-lethal, and lethal weapons, running the gamut from cattle prods to sub-machine guns to bows and arrows.

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.

Actual letters written to the leading hackers' magazine For 25 years, 2600: The Hacker Quarterly has given voice to the hacker community in all its manifestations. This collection of letters to the magazine reveals the thoughts and viewpoints of hackers, both white and black hat, as well as hacker wannabes, technophiles, and people concerned about computer security. Insightful and entertaining, the exchanges illustrate 2600's vast readership, from teenage rebels, anarchists, and survivalists to law enforcement, consumer advocates, and worried parents. Dear Hacker is must reading for technology aficionados, 2600's wide and loyal audience, and anyone seeking entertainment well laced with insight into our society. Coverage Includes: Question Upon Question Tales from the Retail Front The Challenges of Life as a Hacker Technology The Magic of the Corporate World Our Biggest Fans Behind the Walls A Culture of Rebels Strange Ramblings For more information and sample letters, check out the companion site at http://lp.wileypub.com/dearhacker/

The conservative columnist shares her thoughts on topics from political correctness and foreign policy to the media, in a collection of her commentaries accompanied by responses from readers on both sides of the political spectrum.

If you want to experiment with radio frequency identification (RFID), this book is the perfect place to start. All you need is some experience with Arduino and Processing, the ability to connect basic circuits on a breadboard with jumper wire—and you're good to go. You'll be guided through three hands-on projects that let you experience RFID in action. RFID is used in various applications, such as identifying store items or accessing a toll road with an EZPass system. After you build each of the book's projects in succession, you'll have the knowledge to pursue RFID applications of your own. Use Processing to get a sense of how RFID readers behave Connect Arduino to an RFID reader and discover how to use RFID tags as keys Automate your office or home, using RFID to turn on systems when you're present, and turn them off when you leave Get a complete list of materials you need, along with code samples and helpful illustrations Tackle each project with easy-to-follow explanations of how the code works