

Hacker Hoaxer Whistleblower Spy The Many Faces Of Anonymous

Eventually, you will extremely discover a additional experience and realization by spending more cash. yet when? complete you give a positive response that you require to get those every needs following having significantly cash? Why dont you attempt to acquire something basic in the beginning? Thats something that will lead you to comprehend even more regarding the globe, experience, some places, in the manner of history, amusement, and a lot more?

It is your extremely own epoch to play in reviewing habit. in the course of guides you could enjoy now is **Hacker Hoaxer Whistleblower Spy The Many Faces Of Anonymous** below.

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

Reset Ronald J. Deibert 2020-09-29 In the 2020 CBC Massey Lectures, bestselling author and renowned technology and security expert Ronald J. Deibert exposes the disturbing influence and impact of the internet on politics, the economy, the environment, and humanity. Digital technologies have given rise to a new machine-based civilization that is increasingly linked to a growing number of social and political maladies. Accountability is weak and insecurity is endemic, creating disturbing opportunities for exploitation. Drawing from the cutting-edge research of the Citizen Lab, the world-renowned digital security research group which he founded and directs, Ronald J. Deibert exposes the impacts of this communications ecosystem on civil society. He tracks a mostly unregulated surveillance industry, innovations in technologies of remote control, superpower policing practices, dark PR firms, and highly profitable hack-for-hire services feeding off rivers of poorly secured personal data. Deibert also unearths how dependence on social media and its expanding universe of consumer electronics creates immense pressure on the natural environment. In order to combat authoritarian practices, environmental degradation, and rampant electronic consumerism, he urges restraints on tech platforms and governments to reclaim the internet for civil society.

Hacked Transmissions Alessandra Renzi 2020-03-24 Mapping the transformation of media activism from the seventies to the present day Hacked Transmissions is a pioneering exploration of how social movements change across cycles of struggle and alongside technology. Weaving a rich fabric of local and international social movements and media practices, politicized hacking, and independent cultural production, it takes as its entry point a multiyear ethnography of Telestreet, a network of pirate television channels in Italy that combined emerging technologies with the medium of television to challenge the media monopoly of tycoon-turned-prime minister Silvio Berlusconi. Street televisions in Italy represented a unique experiment in combining old and new media to forge grassroots alliances, fight social isolation, and build more resilient communities. Alessandra Renzi digs for the roots of Telestreet in

movements of the 1970s and the global activism of the 1990s to trace its transformations in the present work of one of the network's more active nodes, insu^tv, in Naples. In so doing, she offers a comprehensive account of transnational media activism, with particular attention to the relations among groups and projects, their modes of social reproduction, the contexts giving rise to them, and the technology they adopt—from zines and radios to social media. Hacked Transmissions is also a study in method, providing examples of co-research between activist researchers and social movements, and a theoretical framework that captures the complexities of grassroots politics and the agency of technology. Providing a rare and timely glimpse into a key activist/media project of the twenty-first century, Hacked Transmissions marks a vital contribution to debates in a range of fields, including media and communication studies, anthropology, science and technology studies, social movements studies, sociology, and cultural theory.

Present Shock Douglas Rushkoff 2014-02-25 People spent the twentieth century obsessed with the future. We created technologies that would help connect us faster, gather news, map the planet, and compile knowledge. We strove for an instantaneous network where time and space could be compressed. Well, the future's arrived. We live in a continuous now enabled by Twitter, email, and a so-called real-time technological shift. Yet this "now" is an elusive goal that we can never quite reach. And the dissonance between our digital selves and our analog bodies has thrown us into a new state of anxiety: present shock.

The WikiLeaks Files WikiLeaks 2015-09-15 What Cablegate tells us about the reach and ambitions of US Empire. Published in collaboration with WikiLeaks. WikiLeaks came to prominence in 2010 with the release of 251,287 top-secret State Department cables, which revealed to the world what the US government really thinks about national leaders, friendly dictators, and supposed allies. It brought to the surface the dark truths of crimes committed in our name: human rights violations, covert operations, and cover-ups. The WikiLeaks Files exposes the machinations of the United States as it imposes a new form of imperialism on the world, one founded on tactics from torture to military action, to trade deals and "soft power," in the perpetual pursuit of expanding influence. The book also includes an introduction by Julian Assange examining the ongoing debates about freedom of information, international surveillance, and justice. An introduction by Julian Assange—writing on the subject for the first time—exposes the ongoing debates about freedom of information, international surveillance, and justice. With contributions by Dan Beeton, Phyllis Bennis, Michael Busch, Peter Certo, Conn Hallinan, Sarah Harrison, Richard Heydarian, Dahr Jamail, Jake Johnston, Alexander Main, Robert Naiman, Francis Njubi Nesbitt, Linda Pearson, Gareth Porter, Tim Shorrock, Russ Wellen, and Stephen Zunes.

This Is an Uprising Mark Engler 2016-02-09 Strategic nonviolent action has reasserted itself as a potent force in shaping public debate and forcing political change. Whether it is an explosive surge of protest calling for racial justice in the United States, a demand for democratic reform in Hong Kong or Mexico, a wave of uprisings against dictatorship in the Middle East, or a tent city on Wall Street that spreads throughout the country, when mass movements erupt onto our television screens, the media portrays them as being as spontaneous and unpredictable. In This is an Uprising, political analysts Mark and Paul Engler uncover the organization and well-planned strategies behind such outbursts of protest, examining core

principles that have been used to spark and guide moments of transformative unrest. This is an Uprising traces the evolution of civil resistance, providing new insights into the contributions of early experimenters such as Mohandas Gandhi and Martin Luther King Jr., groundbreaking theorists such as Gene Sharp and Frances Fox Piven, and contemporary practitioners who have toppled repressive regimes in countries such as South Africa, Serbia, and Egypt. Drawing from discussions with activists now working to defend human rights, challenge corporate corruption, and combat climate change, the Englers show how people with few resources and little influence in conventional politics can nevertheless engineer momentous upheavals. Although it continues to prove its importance in political life, the strategic use of nonviolent action is poorly understood.

Nonviolence is usually studied as a philosophy or moral code, rather than as a method of political conflict, disruption, and escalation. This is an Uprising corrects this oversight. It argues that if we are always taken by surprise by dramatic outbreaks of revolt, and if we decline to incorporate them into our view of how societies progress, then we pass up the chance to fully grasp a critical phenomenon—and to harness its power to create lasting change.

Revolution in the Age of Social Media Linda Herrera 2014-07-22 Egypt's January 25 revolution was triggered by a Facebook page and played out both in virtual spaces and the streets. Social media serves as a space of liberation, but it also functions as an arena where competing forces vie over the minds of the young as they battle over ideas as important as the nature of freedom and the place of the rising generation in the political order. This book provides piercing insights into the ongoing struggles between people and power in the digital age.

Networking Peripheries Anita Say Chan 2014-01-31 An exploration of the diverse experiments in digital futures as they advance far from the celebrated centers of technological innovation and entrepreneurship. In *Networking Peripheries*, Anita Chan shows how digital cultures flourish beyond Silicon Valley and other celebrated centers of technological innovation and entrepreneurship. The evolving digital cultures in the Global South vividly demonstrate that there are more ways than one to imagine what digital practice and global connection could look like. To explore these alternative developments, Chan investigates the diverse initiatives being undertaken to “network” the nation in contemporary Peru, from attempts to promote the intellectual property of indigenous artisans to the national distribution of digital education technologies to open technology activism in rural and urban zones. Drawing on ethnographic accounts from government planners, regional free-software advocates, traditional artisans, rural educators, and others, Chan demonstrates how such developments unsettle dominant conceptions of information classes and innovations zones. Government efforts to turn rural artisans into a new creative class progress alongside technology activists' efforts to promote indigenous rights through information tactics; plans pressing for the state wide adoption of open source-based technologies advance while the One Laptop Per Child initiative aims to network rural classrooms by distributing laptops. As these cases show, the digital cultures and network politics emerging on the periphery do more than replicate the technological future imagined as universal from the center.

Occult Features of Anarchism Erica Lagalisse 2019-02-01 In the nineteenth century anarchists were accused of conspiracy by governments afraid of revolution, but in the current century various “conspiracy theories” suggest that anarchists are controlled by government itself. The Illuminati were a network of intellectuals who argued for self-government and against private property, yet the public is now often told that they were (and are) the very group that controls governments and defends private property around the world. Intervening in such misinformation, Lagalisse works with primary and secondary sources in multiple languages to set straight the history of the Left and illustrate the actual relationship between revolutionism, pantheistic occult philosophy, and the clandestine fraternity. Exploring hidden correspondences between anarchism, Renaissance magic, and New Age movements, Lagalisse also advances critical scholarship regarding leftist attachments to secular politics. Inspired by

anthropological fieldwork within today's anarchist movements, her essay challenges anarchist atheism insofar as it poses practical challenges for coalition politics in today's world. Studying anarchism as a historical object, *Occult Features of Anarchism* also shows how the development of leftist theory and practice within clandestine masculine public spheres continues to inform contemporary anarchist understandings of the “political,” in which men's oppression by the state becomes the prototype for power in general. Readers behold how gender and religion become privatized in radical counterculture, a historical process intimately linked to the privatization of gender and religion by the modern nation-state.

Digital Democracy, Social Media and Disinformation Petros Iosifidis 2020-12-31 *Digital Democracy, Social Media and Disinformation* discusses some of the political, regulatory and technological issues which arise from the increased power of internet intermediaries (such as Facebook, Twitter and YouTube) and the impact of the spread of digital disinformation, especially in the midst of a health pandemic. The volume provides a detailed account of the main areas surrounding digital democracy, disinformation and fake news, freedom of expression and post-truth politics. It addresses the major theoretical and regulatory concepts of digital democracy and the ‘network society’ before offering potential socio-political and technological solutions to the fight against disinformation and fake news. These solutions include self-regulation, rebuttals and myth-busting, news literacy, policy recommendations, awareness and communication strategies and the potential of recent technologies such as the blockchain and public interest algorithms to counter disinformation. After addressing what has currently been done to combat disinformation and fake news, the volume argues that digital disinformation needs to be identified as a multifaceted problem, one that requires multiple approaches to resolve. Governments, regulators, think tanks, the academy and technology providers need to take more steps to better shape the next internet with as little digital disinformation as possible by means of a regional analysis. In this context, two cases concerning Russia and Ukraine are presented regarding disinformation and the ways it was handled. Written in a clear and direct style, this volume will appeal to students and researchers within the social sciences, computer science, law and business studies, as well as policy makers engaged in combating what constitutes one of the most pressing issues of the digital age.

Big Money Thinks Small Joel Tillinghast 2017-08-15 Market mistakes to avoid: “Written for investors at all levels...[a] practical, no-nonsense guide.”—Publishers Weekly One of Money Week's Five Best Books of the Year Investors are tempted daily by misleading or incomplete information. They may make a lucky bet, realize a sizable profit, and find themselves full of confidence. Their next high-stakes gamble might backfire, not only hitting them in the balance sheet but also taking a mental and emotional toll. Even veteran investors can be caught off guard: a news item may suddenly cause havoc for an industry they've invested in; crowd mentality among fellow investors may skew the market; a CEO may turn out to be unprepared to effectively guide a company. How can one stay focused in such a volatile world? If you can't trust your past successes to plan and predict, how can you avoid risky situations in the future? Patience and methodical planning will pay far greater dividends than flashy investments. In *Big Money Thinks Small*, veteran fund manager Joel Tillinghast shows investors how to avoid making these mistakes. He offers a set of simple but crucial steps to successful investing, including: · Know yourself, how you arrive at decisions, and how you might be susceptible to self-deception · Make decisions based on your own expertise, and do not invest in what you don't understand · Select only trustworthy and capable colleagues and collaborators · Learn how to identify and avoid investments with inherent flaws · Always search for bargains, and never forget that the first responsibility of an investor is to identify mispriced stocks

The Many Faces of Josephine Baker Peggy Caravantes 2015-02-01 With determination and audacity, Josephine Baker exploited her comic and musical abilities to become a worldwide icon of the Jazz Age. *The Many Faces of Josephine Baker: Dancer, Singer, Activist, Spy* provides the first in-depth portrait of this remarkable

woman for young adults. Digging beneath the sensationalism usually associated with Baker and her uninhibited dancing, author Peggy Caravantes follows Baker's remarkable life from her childhood in the depths of poverty, to her comedic rise in vaudeville, to fame in Europe, outspoken participation in the US Civil Rights Movement, espionage work for the French Resistance during World War II, and adoption of 12 children, each from a different nationality, ethnicity, or religious group—her "rainbow tribe." Also included are informative sidebars on relevant topics such as the 1917 East St. Louis riot, Pullman railway porters, the Charleston, and more; lush photographs; an appendix updating readers on the lives of the rainbow tribe; and source notes and a bibliography, making this a must-have resource for any student, Baker fan, or history buff. Peggy Caravantes is a former English and history teacher, middle school principal, and deputy school superintendent. She is the author of 16 books for middle grades and young adult readers, including *Petticoat Spies: Six Women Spies of the Civil War* and *American Hero: The Audie Murphy Story*. Her YA biographies have been selected for the California Titles for Young Adults, Tri-State Books of Note, and the Top Forty Young Adult Nonfiction Books lists. She lives in San Antonio, Texas.

Understanding E-Governance for Development Richard Heeks 2020 New information and communication technologies can make a significant contribution to the achievement of good governance goals. This 'e-governance' can make governance more efficient and more effective, and bring other benefits too. This paper outlines the three main contributions of e-governance: improving government processes (e-administration); connecting citizens (e-citizens and e-services); and building external interactions (e-society). Case studies are used to show that e-governance is a current, not just future, reality for developing countries. However, most e-governance initiatives fail. Countries therefore face two challenges. First, the strategic challenge of e-readiness: preparing six identified pre-conditions for e-governance. Second, the tactical challenge of closing design -- reality gaps: adopting best practice in e-governance projects in order to avoid failure and to achieve success. A vision for change is therefore outlined of which more details are given in a related paper.

Hacker, Hoaxer, Whistleblower, Spy Gabriella Coleman 2015-10-06 Here is the ultimate book on the worldwide movement of hackers, pranksters, and activists that operates under the non-name Anonymous, by the writer the Huffington Post says "knows all of Anonymous' deepest, darkest secrets." Half a dozen years ago, anthropologist Gabriella Coleman set out to study the rise of this global phenomenon just as some of its members were turning to political protest and dangerous disruption (before Anonymous shot to fame as a key player in the battles over WikiLeaks, the Arab Spring, and Occupy Wall Street). She ended up becoming so closely connected to Anonymous that the tricky story of her inside-outside status as Anon confidante, interpreter, and erstwhile mouthpiece forms one of the themes of this witty and entirely engrossing book. The narrative brims with details unearthed from within a notoriously mysterious subculture, whose semi-legendary tricksters—such as Topiary, tflow, Anachaos, and Sabu—emerge as complex, diverse, politically and culturally sophisticated people. Propelled by years of chats and encounters with a multitude of hackers, including imprisoned activist Jeremy Hammond and the double agent who helped put him away, Hector Monsegur, *Hacker, Hoaxer, Whistleblower, Spy* is filled with insights into the meaning of digital activism and little understood facets of culture in the Internet age, including the history of "trolling," the ethics and metaphysics of hacking, and the origins and manifold meanings of "the lulz."

CUCKOO'S EGG Clifford Stoll 2012-05-23 Before the Internet became widely known as a global tool for terrorists, one perceptive U.S. citizen recognized its ominous potential. Armed with clear evidence of computer espionage, he began a highly personal quest to expose a hidden network of spies that threatened national security. But would the authorities back him up? Cliff Stoll's dramatic firsthand account is "a computer-age detective story, instantly fascinating [and] astonishingly gripping" (Smithsonian). Cliff Stoll was an astronomer turned systems manager at Lawrence

Berkeley Lab when a 75-cent accounting error alerted him to the presence of an unauthorized user on his system. The hacker's code name was "Hunter"—a mysterious invader who managed to break into U.S. computer systems and steal sensitive military and security information. Stoll began a one-man hunt of his own: spying on the spy. It was a dangerous game of deception, broken codes, satellites, and missile bases—a one-man sting operation that finally gained the attention of the CIA . . . and ultimately trapped an international spy ring fueled by cash, cocaine, and the KGB.

Secrets and Lies Bruce Schneier 2015-03-23 This anniversary edition which has stood the test of time as a runaway best-seller provides a practical, straightforward guide to achieving security throughout computer networks. No theory, no math, no fiction of what should be working but isn't, just the facts. Known as the master of cryptography, Schneier uses his extensive field experience with his own clients to dispel the myths that often mislead IT managers as they try to build secure systems. A much-touted section: Schneier's tutorial on just what cryptography (a subset of computer security) can and cannot do for them, has received far-reaching praise from both the technical and business community. Praise for *Secrets and Lies* "This is a business issue, not a technical one, and executives can no longer leave such decisions to techies. That's why *Secrets and Lies* belongs in every manager's library."—Business Week "Startlingly lively....a jewel box of little surprises you can actually use."—Fortune "Secrets is a comprehensive, well-written work on a topic few business leaders can afford to neglect."—Business 2.0 "Instead of talking algorithms to geeky programmers, [Schneier] offers a primer in practical computer security aimed at those shopping, communicating or doing business online—almost everyone, in other words."—The Economist "Schneier...peppers the book with lively anecdotes and aphorisms, making it unusually accessible."—Los Angeles Times With a new and compelling Introduction by the author, this premium edition will become a keepsake for security enthusiasts of every stripe.

My Life as a Night Elf Priest Bonnie Nardi 2010-06-02 "Ever since the creators of the animated television show South Park turned their lovingly sardonic gaze on the massively multiplayer online game World of Warcraft for an entire episode, WoW's status as an icon of digital culture has been secure. My Life as a Night Elf Priest digs deep beneath the surface of that icon to explore the rich particulars of the World of Warcraft player's experience." —Julian Dibbell, Wired "World of Warcraft is the best representative of a significant new technology, art form, and sector of society: the theme-oriented virtual world. Bonnie Nardi's pioneering transnational ethnography explores this game both sensitively and systematically using the methods of cultural anthropology and aesthetics with intensive personal experience as a guild member, media teacher, and magical quest Elf." —William Sims Bainbridge, author of *The Warcraft Civilization* and editor of *Online Worlds* "Nardi skillfully covers all of the hot button issues that come to mind when people think of video games like World of Warcraft such as game addiction, sexism, and violence. What gives this book its value are its unexpected gems of rare and beautifully detailed research on less sensationalized topics of interest such as the World of Warcraft player community in China, game modding, the increasingly blurred line between play and work, and the rich and fascinating lives of players and player cultures. Nardi brings World of Warcraft down to earth for non-players and ties it to social and cultural theory for scholars. . . . the best ethnography of a single virtual world produced so far." —Lisa Nakamura, University of Illinois World of Warcraft rapidly became one of the most popular online world games on the planet, amassing 11.5 million subscribers—officially making it an online community of gamers that had more inhabitants than the state of Ohio and was almost twice as populous as Scotland. It's a massively multiplayer online game, or MMO in gamer jargon, where each person controls a single character inside a virtual world, interacting with other people's characters and computer-controlled monsters, quest-givers, and merchants. In *My Life as a Night Elf Priest*, Bonnie Nardi, a well-known ethnographer who has published extensively on how theories of what we do intersect with how we adopt and use technology, compiles more than three years of

participatory research in Warcraft play and culture in the United States and China into this field study of player behavior and activity. She introduces us to her research strategy and the history, structure, and culture of Warcraft; argues for applying activity theory and theories of aesthetic experience to the study of gaming and play; and educates us on issues of gender, culture, and addiction as part of the play experience. Nardi paints a compelling portrait of what drives online gamers both in this country and in China, where she spent a month studying players in Internet cafes. Bonnie Nardi has given us a fresh look not only at World of Warcraft but at the field of game studies as a whole. One of the first in-depth studies of a game that has become an icon of digital culture, *My Life as a Night Elf Priest* will capture the interest of both the gamer and the ethnographer. Bonnie A. Nardi is an anthropologist by training and a professor in the Department of Informatics in the Donald Bren School of Information and Computer Sciences at the University of California, Irvine. Her research focus is the social implications of digital technologies. She is the author of *A Small Matter of Programming: Perspectives on End User Computing* and the coauthor of *Information Ecologies: Using Technology with Heart* and *Acting with Technology: Activity Theory and Interaction Design*. Cover art by Jessica Damsky

Exploding the Phone Phil Lapsley 2013-02-05 "A rollicking history of the telephone system and the hackers who exploited its flaws." -Kirkus Reviews, starred review Before smartphones, back even before the Internet and personal computers, a misfit group of technophiles, blind teenagers, hippies, and outlaws figured out how to hack the world's largest machine: the telephone system. Starting with Alexander Graham Bell's revolutionary "harmonic telegraph," by the middle of the twentieth century the phone system had grown into something extraordinary, a web of cutting-edge switching machines and human operators that linked together millions of people like never before. But the network had a billion-dollar flaw, and once people discovered it, things would never be the same. *Exploding the Phone* tells this story in full for the first time. It traces the birth of long-distance communication and the telephone, the rise of AT&T's monopoly, the creation of the sophisticated machines that made it all work, and the discovery of Ma Bell's Achilles' heel. Phil Lapsley expertly weaves together the clandestine underground of "phone phreaks" who turned the network into their electronic playground, the mobsters who exploited its flaws to avoid the feds, the explosion of telephone hacking in the counterculture, and the war between the phreaks, the phone company, and the FBI. The product of extensive original research, *Exploding the Phone* is a groundbreaking, captivating book that "does for the phone phreaks what Steven Levy's *Hackers* did for computer pioneers" (Boing Boing). "An authoritative, jaunty and enjoyable account of their sometimes comical, sometimes impressive and sometimes disquieting misdeeds." -The Wall Street Journal "Brilliantly researched." -The Atlantic "A fantastically fun romp through the world of early phone hackers, who sought free long distance, and in the end helped launch the computer era." -The Seattle Times

The Art of Deception Kevin D. Mitnick 2011-08-04 The world's most infamous hacker offers an insider's view of the low-tech threats to high-tech security Kevin Mitnick's exploits as a cyber-desperado and fugitive form one of the most exhaustive FBI manhunts in history and have spawned dozens of articles, books, films, and documentaries. Since his release from federal prison, in 1998, Mitnick has turned his life around and established himself as one of the most sought-after computer security experts worldwide. Now, in *The Art of Deception*, the world's most notorious hacker gives new meaning to the old adage, "It takes a thief to catch a thief." Focusing on the human factors involved with information security, Mitnick explains why all the firewalls and encryption protocols in the world will never be enough to stop a savvy grifter intent on rifling a corporate database or an irate employee determined to crash a system. With the help of many fascinating true stories of successful attacks on business and government, he illustrates just how susceptible even the most locked-down information systems are to a slick con artist impersonating an IRS agent. Narrating from the points of view of both the

attacker and the victims, he explains why each attack was so successful and how it could have been prevented in an engaging and highly readable style reminiscent of a true-crime novel. And, perhaps most importantly, Mitnick offers advice for preventing these types of social engineering hacks through security protocols, training programs, and manuals that address the human element of security.

The Ten-Cent Plague David Hajdu 2009-02-03 Examines the influence of comic books on the evolution of American popular culture in the years between World War II and the emergence of television, focusing on the battle against comic books by church groups, community elite, and a right-wing Congress.

Respawn Colin Milburn 2018-12-14 In *Respawn* Colin Milburn examines the connections between video games, hacking, and science fiction that galvanize technological activism and technological communities. Discussing a wide range of games, from *Portal* and *Final Fantasy VII* to *Super Mario Sunshine* and *Shadow of the Colossus*, Milburn illustrates how they impact the lives of gamers and non-gamers alike. They also serve as resources for critique, resistance, and insurgency, offering a space for players and hacktivist groups such as Anonymous to challenge obstinate systems and experiment with alternative futures. Providing an essential walkthrough guide to our digital culture and its high-tech controversies, Milburn shows how games and playable media spawn new modes of engagement in a computerized world.

Coding Democracy Maureen Webb 2021-07-27 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.

Pirate Politics Patrick Burkart 2014-01-24 An examination of the Pirate political movement in Europe analyzes its advocacy for free expression and the preservation of the Internet as a commons.

The Cybersecurity Dilemma Ben Buchanan 2017-02-01 Why do nations break into one another's most important computer networks? There is an obvious answer: to steal valuable information or to attack. But this isn't the full story. This book draws on often-overlooked documents leaked by Edward Snowden, real-world case studies of cyber operations, and policymaker perspectives to show that intruding into other countries' networks has enormous defensive value as well. Two nations, neither of which seeks to harm the other but neither of which trusts the other, will often find it prudent to launch intrusions. This general problem, in which a nation's means of securing itself threatens the security of others and risks escalating tension, is a bedrock concept in international relations and is called the 'security dilemma'. This book shows not only that the security dilemma applies to cyber operations, but also that the particular characteristics of the digital domain mean that the effects are deeply pronounced. The cybersecurity dilemma is both a vital concern of modern statecraft and a means of accessibly understanding the essential components of cyber operations.

Sandworm Andy Greenberg 2020-10-20 Originally published in hardcover in 2019 by Doubleday.

We Are Anonymous Parmy Olson 2012-06-05 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.

Networked Press Freedom Mike Ananny 2018-05-04

Reimagining press freedom in a networked era: not just a journalist's right to speak but also a public's right to hear. In *Networked Press Freedom*, Mike Ananny offers a new way to think about freedom of the press in a time when media systems are in fundamental flux. Ananny challenges the idea that press freedom comes only from heroic, lone journalists who speak truth to power. Instead, drawing on journalism studies, institutional sociology, political theory, science and technology studies, and an analysis of ten years of journalism discourse about news and technology, he argues that press freedom emerges from social, technological, institutional, and normative forces that vie for power and fight for visions of democratic life. He shows how dominant, historical ideals of professionalized press freedom often mistook journalistic freedom from constraints for the public's freedom to encounter the rich mix of people and ideas that self-governance requires. Ananny's notion of press freedom ensures not only an individual right to speak, but also a public right to hear. Seeing press freedom as essential for democratic self-governance, Ananny explores what publics need, what kind of free press they should demand, and how today's press freedom emerges from intertwined collections of humans and machines. If someone says, "The public needs a free press," Ananny urges us to ask in response, "What kind of public, what kind of freedom, and what kind of press?" Answering these questions shows what robust, self-governing publics need to demand of technologists and journalists alike.

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

Renegade Dreams Laurence Ralph 2014-09-15 Inner city communities in the US have become "junkyards of dreams," to quote Mike Davis—wastelands where gangs package narcotics to stimulate the local economy, gunshots occur multiple times on any given day, and dreams of a better life can fade into the realities of poverty and disability. Laurence Ralph lived in such a community in Chicago for three years, conducting interviews and participating in meetings with members of the local gang which has been central to the community since the 1950s. Ralph discovered that the experience of injury, whether physical or social, doesn't always crush dreams into oblivion; it can transform them into something

productive: renegade dreams. The first part of this book moves from a critique of the way government officials, as opposed to grandmothers, have been handling the situation, to a study of the history of the historic "Divine Knights" gang, to a portrait of a duo of gang members who want to be recognized as "authentic" rappers (they call their musical style "crack music") and the difficulties they face in exiting the gang. The second part is on physical disability, including being wheelchair bound, the prevalence of HIV/AIDS among heroin users, and the experience of brutality at the hands of Chicago police officers. In a final chapter, "The Frame, Or How to Get Out of an Isolated Space," Ralph offers a fresh perspective on how to understand urban violence. The upshot is a total portrait of the interlocking complexities, symbols, and vicissitudes of gang life in one of the most dangerous inner city neighborhoods in the US. We expect this study will enjoy considerable readership, among anthropologists, sociologists, and other scholars interested in disability, urban crime, and race.

Revenue Operations Stephen G. Diorio 2022-04-19 Crush siloes by connecting teams, data, and technologies with a new systems-based approach to growth. Growing a business in the 21st Century has become a capital intensive and data-driven team sport. In *Revenue Operations: A New Way to Align Sales and Marketing, Monetize Data, and Ignite Growth*, an accomplished team of practitioners, academics, and experts provide a proven system for aligning revenue teams and unlocking growth. The book shows everyone how to connect the dots across an increasingly complex technology ecosystem to simplify selling and accelerate revenue expansion. With *Revenue Operations*, you'll understand what it takes to successfully transition to the new system of growth without killing your existing business. This practical and executable approach can be used by virtually any business - large or small, regardless of history or industry - that wants to generate more growth and value. By reading this book you will find: Real-world case studies and personal experiences from executives across an array of high technology, commercial, industrial, services, consumer, and cloud-based businesses. The six core elements of a system for managing your commercial operations, digital selling infrastructure, and customer data assets. Nine building-blocks that connect the dots across your sales and marketing technology ecosystem to generate more consistent growth and a better customer experience at lower costs. The skills and tools that next generation growth leaders will need to chart the roadmap for a successful career in any growth discipline for the next 25 years. An indispensable resource for anyone who wants to get more from their business - board members, CEOs, business unit leaders, strategists, thought leaders, analysts, operations professionals, partners, and front-line doers in sales, marketing, and service - *Revenue Operations* is based on over one thousand surveys of and interviews with business professionals conducted during 2020 and 2021. It also includes a comprehensive analysis of the sales and marketing technology landscape. As a perfectly balanced combination of academic insight and data-driven application, this book belongs on the bookshelves of anyone responsible for driving revenue and growth.

Underground Suelette Dreyfus 2012-01-05 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.

Low Power to the People Christina Dunbar-Hester 2014-11-14 An examination of how activists combine political advocacy and technical practice in their promotion of the emancipatory potential of local low-power FM radio. The United States ushered in a new era of small-scale broadcasting in 2000 when it began issuing low-power FM (LPFM) licenses for noncommercial

radio stations around the country. Over the next decade, several hundred of these newly created low-wattage stations took to the airwaves. In *Low Power to the People*, Christina Dunbar-Hester describes the practices of an activist organization focused on LPFM during this era. Despite its origins as a pirate broadcasting collective, the group eventually shifted toward building and expanding regulatory access to new, licensed stations. These radio activists consciously cast radio as an alternative to digital utopianism, promoting an understanding of electronic media that emphasizes the local community rather than a global audience of Internet users. Dunbar-Hester focuses on how these radio activists impute emancipatory politics to the "old" medium of radio technology by promoting the idea that "microradio" broadcasting holds the potential to empower ordinary people at the local community level. The group's methods combine political advocacy with a rare commitment to hands-on technical work with radio hardware, although the activists' hands-on, inclusive ethos was hampered by persistent issues of race, class, and gender. Dunbar-Hester's study of activism around an "old" medium offers broader lessons about how political beliefs are expressed through engagement with specific technologies. It also offers insight into contemporary issues in media policy that is particularly timely as the FCC issues a new round of LPFM licenses.

The Charisma Machine Morgan G. Ames 2019-11-19 A fascinating examination of technological utopianism and its complicated consequences. In *The Charisma Machine*, Morgan Ames chronicles the life and legacy of the One Laptop per Child project and explains why—despite its failures—the same utopian visions that inspired OLPC still motivate other projects trying to use technology to "disrupt" education and development. Announced in 2005 by MIT Media Lab cofounder Nicholas Negroponte, One Laptop per Child promised to transform the lives of children across the Global South with a small, sturdy, and cheap laptop computer, powered by a hand crank. In reality, the project fell short in many ways—starting with the hand crank, which never materialized. Yet the project remained charismatic to many who were captivated by its claims of access to educational opportunities previously out of reach. Behind its promises, OLPC, like many technology projects that make similarly grand claims, had a fundamentally flawed vision of who the computer was made for and what role technology should play in learning. Drawing on fifty years of history and a seven-month study of a model OLPC project in Paraguay, Ames reveals that the laptops were not only frustrating to use, easy to break, and hard to repair, they were designed for "technically precocious boys"—idealized younger versions of the developers themselves—rather than the children who were actually using them. *The Charisma Machine* offers a cautionary tale about the allure of technology hype and the problems that result when utopian dreams drive technology development.

Coding Freedom E. Gabriella Coleman 2013 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.

Countdown to Zero Day Kim Zetter 2014-11-11 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.

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

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

The Snowden Files Luke Harding 2014-02-07 Now a major motion picture, directed by Oliver Stone and starring Joseph Gordon-Levitt. Edward Snowden was a 29-year-old

computer genius working for the National Security Agency when he shocked the world by exposing the near-universal mass surveillance programs of the United States government. His whistleblowing has shaken the leaders of nations worldwide, and generated a passionate public debate on the dangers of global monitoring and the threat to individual privacy. In a tour de force of investigative journalism that reads like a spy novel, award-winning Guardian reporter Luke Harding tells Snowden's astonishing story—from the day he left his glamorous girlfriend in Honolulu carrying a hard drive full of secrets, to the weeks of his secret-spilling in Hong Kong, to his battle for asylum and his exile in Moscow. For the first time, Harding brings together the many sources and strands of the story—touching on everything from concerns about domestic spying to the complicity of the tech sector—while also placing us in the room with Edward Snowden himself. The result is a gripping insider narrative—and a necessary and timely account of what is at stake for all of us in the new digital age.

The Idealist Justin Peters 2017-01-03 This smart, "riveting" (Los Angeles Times) history of the Internet free culture movement and its larger effects on society—and the life and shocking suicide of Aaron Swartz, a founding developer of Reddit and Creative Commons—written by Slate correspondent Justin Peters "captures Swartz flawlessly" (The New York Times Book Review). Aaron Swartz was a zealous young advocate for the free exchange of information and creative content online. He committed suicide in 2013 after being indicted by the government for illegally downloading millions of academic articles from a nonprofit online database. From the age of fifteen, when Swartz, a computer prodigy, worked with Lawrence Lessig to launch Creative Commons, to his years as a fighter for copyright reform and open information, to his work leading the protests against the Stop Online Piracy Act (SOPA), to his posthumous status as a cultural icon, Swartz's life was inextricably connected to the free culture movement. Now Justin Peters examines Swartz's life in the context of 200 years of struggle over the control of information. In vivid, accessible prose, *The Idealist* situates Swartz in the context of other "data moralists" past and present, from lexicographer Noah Webster to ebook pioneer Michael Hart to NSA whistleblower Edward Snowden. In the process, the book explores the history of copyright statutes and the public domain; examines archivists' ongoing quest to build the "library of the future"; and charts the rise of open access, the copyleft movement, and other ideologies that have come to challenge protectionist intellectual property policies. Peters also breaks down the government's case against Swartz and explains how we reached the point where federally funded academic research came to be considered private property, and downloading that material in bulk came to be considered a federal crime. *The Idealist* is "an excellent survey of the intellectual property battlefield, and a sobering memorial to its most tragic victim" (The Boston Globe) and an essential look at the impact of the free culture movement on our daily lives and on generations to come.

Cult of the Dead Cow Joseph Menn 2019-06-04 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.

Social Engineering Robert W. Gehl 2022-03-08 Manipulative communication—from early twentieth-century propaganda to today's online con artistry—examined through the lens of social engineering. The United States is awash in manipulated information about everything from election results to the effectiveness of medical treatments. Corporate social media is an especially good channel for manipulative communication, with Facebook a particularly willing vehicle for it. In *Social Engineering*, Robert Gehl and Sean Lawson show that online misinformation has its roots in earlier techniques: mass social engineering of the early twentieth century and interpersonal hacker social engineering of the 1970s, converging today into what they call "masspersonal social engineering." As Gehl and Lawson trace contemporary manipulative communication back to earlier forms of social engineering, possibilities for amelioration become clearer. The authors show how specific manipulative communication practices are a mixture of information gathering, deception, and truth-indifferent statements, all with the instrumental goal of getting people to take actions the social engineer wants them to. Yet the term "fake news," they claim, reduces everything to a true/false binary that fails to encompass the complexity of manipulative communication or to map onto many of its practices. They pay special attention to concepts and terms used by hacker social engineers, including the hacker concept of "bullshitting," which the authors describe as a truth-indifferent mix of deception, accuracy, and sociability. They conclude with recommendations for how society can undermine masspersonal social engineering and move toward healthier democratic deliberation.