Hacker Hoaxer Whistleblower Spy The Many Faces Of Anonymous

This is likewise one of the factors by obtaining the soft documents of this **Hacker Hoaxer Whistleblower Spy The Many Faces Of Anonymous** by online. You might not require more become old to spend to go to the ebook establishment as competently as search for them. In some cases, you likewise get not discover the broadcast Hacker Hoaxer Whistleblower Spy The Many Faces Of Anonymous that you are looking for. It will completely squander the time.

However below, behind you visit this web page, it will be thus categorically easy to get as with ease as download lead Hacker Hoaxer Whistleblower Spy The Many Faces Of Anonymous

It will not acknowledge many times as we notify before. You can reach it even if con something else at house and even in your workplace. thus easy! So, are you question? Just exercise just

what we provide under as with ease as evaluation **Hacker Hoaxer Whistleblower Spy The Many Faces Of Anonymous** what you later to read!

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.

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.

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.

The Sherlock Holmes Handbook Ransom Riggs 2010-03-01 Full of fascinating how-to skills and evocative illustrations, this must-have guide will appeal to Baker Street Irregulars of all ages. This reader's companion to the casework of Sherlock Holmes explores the methodology of the world's most famous consulting detective. From analyzing fingerprints and decoding ciphers to creating disguises and faking one's own death, readers will learn how Holmes solved his most celebrated cases—plus an arsenal of modern techniques available to today's armchair sleuths. Along the way, readers will discover a host of trivia about the master detective and his universe: Why did Holmes never marry? How was the real Scotland Yard organized? Was cocaine really legal back then? And why were

the British so terrified of Australia? For die-hardSherlockians and amateur investigators alike, this handbook is nothing less than . . . elementary.

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.

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

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.

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

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.

The Wikileaks Files WikiLeaks 2015-06-02 What Cablegate tells us about the scope of U.S. foreign policy around the world

Sandworm Andy Greenberg 2019-11-05 "With the nuance of a reporter and the pace of a thriller writer, Andy Greenberg gives us a glimpse of the cyberwars of the future while at the same time placing his story in the long arc of Russian and Ukrainian history." —Anne Applebaum, bestselling author of Twilight of Democracy The

true story of the most devastating act of cyberwarfare in history and the desperate hunt to identify and track the elite Russian agents behind it: "[A] chilling account of a Kremlin-led cyberattack, a new front in global conflict" (Financial Times). In 2014, the world witnessed the start of a mysterious series of cyberattacks. Targeting American utility companies, NATO, and electric grids in Eastern Europe, the strikes grew ever more brazen. They culminated in the summer of 2017, when the malware known as NotPetya was unleashed, penetrating, disrupting, and paralyzing some of the world's largest businesses—from drug manufacturers to software developers to shipping companies. At the attack's epicenter in Ukraine, ATMs froze. The railway and postal systems shut down. Hospitals went dark. NotPetya spread around the world, inflicting an unprecedented ten billion dollars in damage—the largest, most destructive cyberattack the world had ever seen. The hackers behind these attacks are quickly gaining a reputation as the most dangerous team of cyberwarriors in history: a group known as Sandworm. Working in the service of Russia's military intelligence agency, they represent a persistent,

highly skilled force, one whose talents are matched by their willingness to launch broad, unrestrained attacks on the most critical infrastructure of their adversaries. They target government and private sector, military and civilians alike. A chilling, globe-spanning detective story, Sandworm considers the danger this force poses to our national security and stability. As the Kremlin's role in foreign government manipulation comes into greater focus, Sandworm exposes the realities not just of Russia's global digital offensive, but of an era where warfare ceases to be waged on the battlefield. It reveals how the lines between digital and physical conflict, between wartime and peacetime, have begun to blur—with world-shaking implications.

Social Media and Democracy Nathaniel Persily 2020-08-31 A state-of-the-art account of what we know and do not know about the effects of digital technology on democracy.

Present Shock Douglas Rushkoff 2013-03-21 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 Social Media Reader Michael Mandiberg 2012-03-01 With the rise of web 2.0 and social media platforms taking over vast tracts of territory on the internet, the media landscape has shifted drastically in the past 20 years, transforming previously stable relationships between media creators and consumers. The Social Media Reader is the first collection to address the collective transformation with pieces on social media, peer production, copyright politics, and other aspects of contemporary internet culture from all the major thinkers in the field. Culling a broad range and incorporating different styles of scholarship from foundational pieces and published articles to unpublished pieces, journalistic accounts, personal narratives from blogs, and whitepapers, The Social Media Reader promises to be an essential text, with contributions from Lawrence Lessig, Henry

Jenkins, Clay Shirky, Tim O'Reilly, Chris Anderson, Yochai Benkler, danah boyd, and Fred von Loehmann, to name a few. It covers a wide-ranging topical terrain, much like the internet itself, with particular emphasis on collaboration and sharing, the politics of social media and social networking, Free Culture and copyright politics, and labor and ownership. Theorizing new models of collaboration, identity, commerce, copyright, ownership, and labor, these essays outline possibilities for cultural democracy that arise when the formerly passive audience becomes active cultural creators, while warning of the dystopian potential of new forms of surveillance and control.

Cyber War Will Not Take Place Thomas Rid 2013 "Published in the United Kingdom in 2013 by C. Hurst & Co. (Publishers) Ltd"--Title page verso.

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.

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.

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.

Hacker, Hoaxer, Whistleblower, Spy Gabriella Coleman 2014-11-04 “Easily the best book on Anonymous.” —Julian Assange. 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."

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, and 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 Christopher Hadnagy 2018-07-31 Harden the human firewall against the most current threats Social Engineering: The Science of Human Hacking reveals the craftier side of the hacker's repertoire—why hack into something when you could just

ask for access? Undetectable by firewalls and antivirus software, social engineering relies on human fault to gain access to sensitive spaces; in this book, renowned expert Christopher Hadnagy explains the most commonly-used techniques that fool even the most robust security personnel, and shows you how these techniques have been used in the past. The way that we make decisions as humans affects everything from our emotions to our security. Hackers, since the beginning of time, have figured out ways to exploit that decision making process and get you to take an action not in your best interest. This new Second Edition has been updated with the most current methods used by sharing stories, examples, and scientific study behind how those decisions are exploited. Networks and systems can be hacked, but they can also be protected; when the “system” in question is a human being, there is no software to fall back on, no hardware upgrade, no code that can lock information down indefinitely. Human nature and emotion is the secret weapon of the malicious social engineering, and this book shows you how to recognize, predict, and prevent this type of manipulation by taking you inside the social engineer’s bag of tricks. Examine the most

common social engineering tricks used to gain access Discover which popular techniques generally don't work in the real world Examine how our understanding of the science behind emotions and decisions can be used by social engineers Learn how social engineering factors into some of the biggest recent headlines Learn how to use these skills as a professional social engineer and secure your company Adopt effective counter-measures to keep hackers at bay By working from the social engineer's playbook, you gain the advantage of foresight that can help you protect yourself and others from even their best efforts. Social Engineering gives you the inside information you need to mount an unshakeable defense.

Cyberwar and Revolution Nick Dyer-Witheford 2019-03-12 Uncovering the class conflicts, geopolitical dynamics, and aggressive capitalism propelling the militarization of the internet Global surveillance, computational propaganda, online espionage, virtual recruiting, massive data breaches, hacked nuclear centrifuges and power grids—concerns about cyberwar have been mounting, rising to a fever pitch after the alleged Russian hacking of the U.S. presidential election and the

Cambridge Analytica scandal. Although cyberwar is widely discussed, few accounts undertake a deep, critical view of its roots and consequences. Analyzing the new militarization of the internet, Cyberwar and Revolution argues that digital warfare is not a bug in the logic of global capitalism but rather a feature of its chaotic, disorderly unconscious. Urgently confronting the concept of cyberwar through the lens of both Marxist critical theory and psychoanalysis, Nick Dyer-Witheford and Svitlana Matviyenko provide a wide-ranging examination of the class conflicts and geopolitical dynamics propelling war across digital networks. Investigating the subjectivities that cyberwar mobilizes, exploits, and bewilders, and revealing how it permeates the fabric of everyday life and implicates us all in its design, this book also highlights the critical importance of the emergent resistance to this digital militarism—hacktivism, digital worker dissent, and off-the-grid activism—for effecting different, better futures.

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, straight-forward 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. **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.

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.

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 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.

We Are Anonymous Parmy Olson 2013-08-04 In January 2012, the hacker collective Anonymous brought down the FBI website in response to planned American laws against internet piracy. In 2011, LulzSec, a sister organisation, broke into and blocked computer systems at VISA, Mastercard and PayPal. The groups have infiltrated the networks of totalitarian governments in Libya and Tunisia. They have attacked the CIA and NATO. But instead of being sanctimonious and

secretive, these cyber activists are flippant and taunting, never hesitating to mock those they've outsmarted. Today, governments, big businesses and social activists are waking up to the true power of the internet, and how it can be manipulated. This is the story of a hive mind, with many hackers across the globe connected to slice through security systems and escape untraced. Through the stories of four key members, We Are Anonymous offers a gripping, adrenalin-fuelled narrative drawing upon extensive research, and hundreds of conversations with the hackers themselves. By coming to know them - their backgrounds, families, motivations - we come to know the human side of their virtual exploits, showing exactly why they're so passionate about disrupting the internet's frontiers.

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.

Radicals Jamie Bartlett 2017-05-18 From the creator of hit podcast The Missing Cryptoqueen _____ 'Thoughtful and intelligent' Observer 'Inside the anti-political revolt that gave us Brexit and Trump' Evening Standard 'Fascinating... Excellent' Literary Review 'Must read ... A radical odyssey' Daily Mail In the last few years the world has changed in unexpected ways. The power of radical ideas and groups is growing. What was once considered extreme is now the mainstream. But what is life like on the political fringes? What is the real power of radicals? Radicals is an exploration of the individuals, groups and movements who are rejecting the way we live now, and attempting to find alternatives.

In it, Jamie Bartlett, one of the world's leading thinkers on radical politics and technology, takes us inside the strange and exciting worlds of the innovators, disruptors, idealists and extremists who think society is broken, and believe they know how to fix it. From dawn raids into open mines to the darkest recesses of the internet, Radicals introduces us to some of the most secretive and influential movements today: techno-futurists questing for immortality, far-right groups seeking to close borders, militant environmentalists striving to save the planet's natural reserves by any means possible, libertarian movements founding new countries, autonomous cooperatives in self-sustaining micro-societies, and psychedelic pioneers attempting to heal society with the help of powerful hallucinogens. As well as providing a fascinating glimpse at the people and ideas driving these groups, Radicals also presents a startling argument: radicals are not only the symptoms of a deep unrest within the world today, but might also offer the most plausible models for our future.

Reset RONALD J. DIEBERT 2021-01-14 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. With COVID-19 only heightening the demand for social media and amplifying negative externalities, it is all the more urgent for us to comprehensively address the intertwined pathologies of social media and surveillance capitalism. This starts with the device in our hand. It's time for us to push RESET.

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.

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.

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.

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.

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.

A for Anonymous David Kushner 2020-03-31 The illustrated, inside story of the legendary hacktivist group's origins and most daring exploits. A for Anonymous shows how a leaderless band of volunteers successfully used hacktivism to fight for the underdog, embarrass their rich and powerful targets--from Sony and Paypal to the Church of Scientology and Ferguson Police Department--all in the name of freedom of speech and

information. Their exploits blurred the distinction between "online" and "reality," and help shape our contemporary world.

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.

The King of Pain Seth Kaufman

2015-04-30 "One of 2012's most enjoyable novels." --Neil Genzlinger, The New York Times "This is a dark, sharp, very funny novel about imprisonment, torture and the dangerous pleasures of stories." --Zoe Heller, Notes on a Scandal A riotously funny portrait of an out-of-control entertainment mogul and a dazzlingly original look at incarceration, The King of Pain is part Jennifer Egan, part Italo Calvino, part "Entourage," and 100% marvelous. Rick Salter is a man everybody loves to hate. But that's fine; in fact, it's become a way of life for Rick ever since the launch of his outrageous – and outrageously successful – reality TV show about torture, The King of Pain. So when one Saturday morning Rick comes to on his living room floor, he's not really bothered that cultural critics have put him on top of the list of "people who will hasten the demise of civilization" – no, his real problem is that he appears to be trapped under his gigantic home entertainment system. Which is no longer attached to the wall, but to him. With no phone or BlackBerry within reach, and with his housekeeper Marta off for the weekend, Rick has 48 long hours ahead of him before he can hope for rescue. 48 hours of pain and bad memories.

Thank god there's a book lying around to pass the time. It's called A History of Prisons and the stories in the book seem to be strangely relevant to Rick's own predicament. "Required reading" --N.Y. Daily News

The Art of Deception Kevin D. Mitnick 2003-10-17 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.