Click Here To Kill Everybody Security And Survival In A Hyper Connected World

How the Original Hacking Supergroup Might Just Save the World
Protocols, Algorithms, and Source Code in C
After the Digital Tornado
Even More Advice from Schneier on Security
Dehumanization and How to Resist It
Protecting Industrial Control Systems from Electronic Threats
An Act of Villainy
Understanding Cyber Conflict
Web Design in a Nutshell
Listening in
Terms of Disservice
Suicide
Cybersecurity in an Insecure Age
Fourteen Analogies
An Amory Ames Mystery
The Beautiful Struggle (Adapted for Young Adults)
Click Here to Kill Everybody
Digital Security in a Networked World
Solving Cyber Risk
Gray Day
The Politics of Infrastructure Security
The Hacking of the American Mind
The Devil's Playbook
How Silicon Valley is Destructive by Design
The Joy of Search
The New Breed
Applied Cryptography
Spam Nation
The Inside Story
An Introduction
Liars and Outliers
The Terrifyingly Real Ways the World Wants You Dead
Facebook
The Forever Decision : for Those Thinking about Suicide and for Those who Know, Love, Or Counsel Them
Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World
The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door
What Doesn't Kill Her
On Cyber
The Hacker and the State

BRONSON MICHAEL

How the Original Hacking Supergroup Might Just Save the World W. W. Norton
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.

Protocols, Algorithms, and Source Code in C Georgetown University Press
This is a frank, compassionate book written to those who contemplate suicide as a way out of their situations. The author issues an invitation to life, helping people accept the imperfections of their lives, and opening eyes to the possibilities of love.
After the Digital Tornado "O'Reilly Media, Inc."
A symbol of modernity, the Viennese Secession was defined by the rebellion of twenty artists who were against the conservative Vienna Künstlerhaus' oppressive influence over the city, the epoch, and the whole Austro-Hungarian Empire. Influenced by Art Nouveau, this movement (created in 1897 by Gustav Klimt, Carl Moll, and Josef Hoffmann) was not an anonymous artistic revolution. Defining itself as a “total art”, without any political or commercial constraint, the Viennese Secession represented the ideological turmoil that affected craftsmen, architects, graphic artists, and designers from this period. Turning away from an established art and immersing themselves in organic, voluptuous, and decorative shapes, these artists opened themselves to an evocative, erotic aesthetic that blatantly offended the bourgeoisie of the time. Painting, sculpture, and architecture are addressed by the authors and highlight the diversity and richness of a movement whose motto proclaimed “for each time its art, for each art its liberty” – a declaration to the innovation and originality of this revolutionary art movement.
Even More Advice from Schneier on Security Cambridge University Press
An examination of how post-9/11 security concerns have transformed the public view and governance of infrastructure. After September 11, 2001, infrastructures—the mundane systems that undergird much of modern life—were suddenly considered “soft targets” that required immediate security

enhancements. Infrastructure protection quickly became the multibillion dollar core of a new and expansive homeland security mission. In this book, Ryan Ellis examines how the long shadow of post-9/11 security concerns have remade and reordered infrastructure, arguing that it has been a stunning transformation. Ellis describes the way workers, civic groups, city councils, bureaucrats, and others used the threat of terrorism as a political resource, taking the opportunity not only to address security vulnerabilities but also to reassert a degree of public control over infrastructure. Nearly two decades after September 11, the threat of terrorism remains etched into the inner workings of infrastructures through new laws, regulations, technologies, and practices. Ellis maps these changes through an examination of three U.S. infrastructures: the postal system, the freight rail network, and the electric power grid. He describes, for example, how debates about protecting the mail from anthrax and other biological hazards spiraled into larger arguments over worker rights, the power of large-volume mailers, and the fortunes of old media in a new media world; how environmental activists leveraged post-9/11 security fears over shipments of hazardous materials to take on the rail industry and the chemical lobby; and how otherwise marginal federal regulators parlayed new mandatory cybersecurity standards for the electric power industry into a robust system of accountability.

Dehumanization and How to Resist It Penguin

How to be a great online searcher, demonstrated with step-by-step searches for answers to a series of intriguing questions (for example, “Is that plant poisonous?”). We all know how to look up something online by typing words into a search engine. We do this so often that we have made the most famous search engine a verb: we Google it—“Japan population” or “Nobel Peace Prize” or “poison ivy” or whatever we want to know. But knowing how to Google something doesn't make us search experts; there's much more we can do to access the massive collective knowledge available online. In The Joy of Search, Daniel Russell shows us how to be great online researchers. We don't have to be computer geeks or a scholar searching out obscure facts; we just need to know some basic methods. Russell demonstrates these methods with step-by-step searches for answers to a series of intriguing questions—from “what is the wrong side of a towel?” to “what is the most likely way you will die?” Along the way, readers will discover essential tools for effective online searches—and learn some fascinating facts and interesting stories. Russell explains how to frame search queries so they will yield information and describes the best ways to use such resources as Google Earth, Google Scholar, Wikipedia, and Wikimedia. He shows when to put search terms in double quotes, how to use the operator (*), why metadata is important, and how to triangulate information from multiple sources. By the end of this engaging journey of discovering, readers will have the definitive answer to why the best online searches involve more than typing a few words into Google.

Protecting Industrial Control Systems from Electronic Threats Yale University Press

For readers of The Second Machine Age or The Soul of an Octopus, a bold, exciting exploration of how building diverse kinds of relationships with robots—inspired by how we interact with animals—could be the key to making our future with robot technology work There has been a lot of ink devoted to discussions of how robots will replace us and take our jobs. But MIT Media Lab researcher and technology policy expert Kate Darling argues just the opposite, suggesting that treating robots with a bit of humanity, more like the way we treat animals, will actually serve us better. From a social, legal, and ethical perspective, she shows that our current ways of thinking don’t leave room for the robot technology that is soon to become part of our everyday routines. Robots are likely to supplement—rather than replace—our own skills and relationships. So if we consider our history of incorporating animals into our work, transportation, military, and even families, we actually have a solid basis for how to contend with this future. A deeply original analysis of our technological future and the ethical dilemmas that await us, The New Breed explains how the treatment of machines can reveal a new understanding of our own history, our own systems, and how we relate—not just to nonhumans, but also to one another.

An Act of Villainy Crown

Designing a new digital social contract for our technological future High technology presents a paradox. In just a few decades, it has transformed the world, making almost limitless quantities of information instantly available to billions of people and reshaping businesses, institutions, and even entire economies. But it also has come to rule our lives, addicting many of us to the march of megapixels across electronic screens both large and small. Despite its undeniable value, technology is exacerbating deep social and political divisions in many societies. Elections influenced by fake news and unscrupulous hidden actors, the cyber-hacking of trusted national institutions, the vacuuming of private information by Silicon Valley behemoths, ongoing threats to vital infrastructure from terrorist groups and even foreign governments—all these concerns are now part of the daily news cycle and are certain to become increasingly serious into the future. In this new world of endless technology, how can individuals, institutions, and governments harness its positive contributions while protecting each of us, no matter who or where we are? In this book, a former Facebook public policy adviser who went on to assist President Obama in the White House offers practical ideas for using technology to create an open and accessible world that protects all consumers and civilians. As a computer scientist turned policymaker, Dipayan Ghosh answers the biggest questions about technology facing the world today. Proving clear and understandable explanations for complex issues, Terms of Disservice will guide industry leaders, policymakers, and the general public as we think about how we ensure that the Internet works for everyone, not just Silicon Valley.

Understanding Cyber Conflict Penguin

On Cyber is a groundbreaking work that fuses information security and military science to lay the foundation of an operational art for cyberspace operations. Hundreds of books have been written on the tactics of cybersecurity and dozens have been written that discuss the strategic implications of cyber conflict. But missing is a book that links the two. On Cyber fills that gap. After millennia of conflict, traditional kinetic war fighting is highly refined and captured in mature and vetted military doctrine. Cyber operations, however is constantly evolving and affords tremendous benefits alongside significant challenges. Nations around the world have raced to build cyber organizations and capabilities, but are struggling to employ cyber operations to their benefit. Some have stumbled, while others have had dramatic impact on the battlefield and global geopolitics. At the same time, companies and even individuals are now facing nation state and nation state enabled threat actors in cyberspace while their governments remain apparently powerless to protect them. Whether you are a network defender or cyber operator, On Cyber is a seminal book and the lessons you learn will help you do your job better. Importantly, network defenders will understand how nation-state threat actors think, organize, operate, and target your organization. Cyber operators will gain a glimpse into the future of cyber doctrine. The authors are perhaps the best two people to author such an ambitious work, having served on the faculty of West Point for a combined 20 years, participated in military cyber operations and training, helped architect the U.S. Army's Cyber Branch, and together possess more than 50 years of military experience.

Web Design in a Nutshell HQN Books

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

Listening in Oxford University Press

Now a New York Times bestseller! There is a Threat Lurking Online with the Power to Destroy Your Finances, Steal Your Personal Data, and Endanger Your Life. In Spam Nation, investigative journalist and cybersecurity expert Brian Krebs unmasks the criminal masterminds driving some of the biggest spam and hacker operations targeting Americans and their bank accounts. Tracing the rise, fall, and alarming resurrection of the digital mafia behind the two largest spam pharmacies-and countless viruses, phishing, and spyware attacks-he delivers the first definitive narrative of the global spam problem and its threat to consumers everywhere. Blending cutting-edge research, investigative reporting, and firsthand interviews, this terrifying true story reveals how we unwittingly invite these digital thieves into our lives every day. From unassuming computer programmers right next door to digital mobsters like "Cosma"-who unleashed a massive malware attack that has stolen thousands of Americans' logins and passwords-Krebs uncovers the shocking lengths to which these people will go to profit from our data and our wallets. Not only are hundreds of thousands of Americans exposing themselves to fraud and dangerously toxic products from rogue online pharmacies, but even those who never open junk messages are at risk. As Krebs notes, spammers can-and do-hack into accounts through these emails, harvest personal information like usernames and passwords, and sell them on the digital black market. The fallout from this global epidemic doesn't just cost consumers and companies billions, it costs lives too. Fast-paced and utterly gripping, Spam Nation ultimately proposes concrete solutions for protecting ourselves online and stemming this tidal wave of cybercrime-before it's too late. "Krebs's talent for exposing the weaknesses in online security has earned him respect in the IT business and loathing among cybercriminals... His track record of scoops...has helped him become the rare blogger who supports himself on the strength of his reputation for hard-nosed reporting." -Bloomberg Businessweek

Terms of Disservice Crown

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.

Suicide John Wiley & Sons

Click Here to Kill Everybody: Security and Survival in a Hyper-connected WorldW. W. Norton & Company

Cybersecurity in an Insecure Age John Wiley & Sons

“Bruce Schneier’s amazing book is the best overview of privacy and security ever written.”—Clay Shirky “Bruce Schneier’s amazing book is the best overview of privacy and security ever written.”—Clay Shirky Your cell phone provider tracks your location and knows who’s with you. Your online and in-store purchasing patterns are recorded, and reveal if you're unemployed, sick, or pregnant. Your e-mails and texts expose your intimate and casual friends. Google knows what you’re thinking because it saves your private searches. Facebook can determine your sexual orientation without you ever mentioning it. The powers that surveil us do more than simply store this information. Corporations use surveillance to manipulate not only the news articles and advertisements we each see, but also the prices we’re offered. Governments use surveillance to discriminate, censor, chill free speech, and put people in danger worldwide. And both sides share this information with each other or, even worse, lose it to cybercriminals in huge data breaches. Much of this is voluntary: we cooperate with corporate surveillance because it promises us convenience, and we submit to government surveillance because it promises us protection. The result is a mass surveillance society of our own making. But have we given up more than we’ve gained? In Data and Goliath, security expert Bruce Schneier offers another path, one that values both security and privacy. He brings his bestseller up-to-date with a new preface covering the latest developments, and then shows us exactly what we can do to reform government surveillance programs, shake up surveillance-based business models, and protect our individual privacy. You'll never look at your phone, your computer, your

credit cards, or even your car in the same way again.
Fourteen Analogies Doubleday
A cybersecurity expert and former Google privacy analyst's urgent call to protect devices and networks against malicious hackers New technologies have provided both incredible convenience and new threats. The same kinds of digital networks that allow you to hail a ride using your smartphone let power grid operators control a country's electricity--and these personal, corporate, and government systems are all vulnerable. In Ukraine, unknown hackers shut off electricity to nearly 230,000 people for six hours. North Korean hackers destroyed networks at Sony Pictures in retaliation for a film that mocked Kim Jong-un. And Russian cyberattackers leaked Democratic National Committee emails in an attempt to sway a U.S. presidential election. And yet despite such documented risks, government agencies, whose investigations and surveillance are stymied by encryption, push for a weakening of protections. In this accessible and riveting read, Susan Landau makes a compelling case for the need to secure our data, explaining how we must maintain cybersecurity in an insecure age.
An Amory Ames Mystery MIT Press
Alex, whose birthday it is, hijacks a story about Birthday Bunny on his special day and turns it into a battle between a supervillain and his enemies in the forest--who, in the original story, are simply planning a surprise party.
The Beautiful Struggle (Adapted for Young Adults) Momentum Press
NEW YORK TIMES EDITORS' CHOICE • Big Tobacco meets Silicon Valley in this "deeply reported and illuminating" (The New York Times Book Review) corporate exposé of what happened when two of the most notorious industries collided—and the vaping epidemic was born. "The best business book I've read since Bad Blood."—Jonathan Eig, New York Times bestselling author of Ali: A Life Howard Willard lusted after Juul. As the CEO of tobacco giant Philip Morris's parent company and a veteran of the industry's long fight to avoid being regulated out of existence, he grew obsessed with a prize he believed could save his company—the e-cigarette, a product with all the addictive upside of the original without the same apparent health risks and bad press. Meanwhile, in Silicon Valley, Adam Bowen and James Monsees began working on a device that was meant to save lives and destroy Big Tobacco, but they ended up baking the industry's DNA into their invention's science and marketing. Ultimately, Juul's e-cigarette was so effective and so market-dominating that it put the company on a collision course with Philip Morris and sparked one of the most explosive public health crises in recent memory. In a deeply reported account, award-winning journalist Lauren Etter tells a riveting story of greed and deception in one of the biggest botched deals in business history. Etter shows how Philip Morris's struggle to innovate left Willard desperate to acquire Juul, even as his own team sounded alarms about the startup's reliance on underage customers. And she shows how Juul's executives negotiated a lavish deal that let them pocket the lion's share of Philip Morris's $12.8 billion investment while government regulators and furious parents mounted a campaign to hold the company's feet to the fire. The Devil's Playbook is the inside story of how Juul's embodiment of Silicon Valley's "move fast and break things" ethos wrought havoc on American health, and how a beleaguered tobacco company was seduced by the promise of a new generation of addicted customers. With both companies' eyes on the financial prize, neither anticipated the sudden outbreak of vaping-linked deaths that would terrorize a nation, crater Juul's value, end Willard's career, and show the costs in human life of the rush to riches—while Juul's founders, board members, and employees walked away with a windfall.
Click Here to Kill Everybody Routledge
Just about any social need is now met with an opportunity to "connect" through digital means. But this convenience is not free—it is purchased with vast amounts of personal data transferred through shadowy backchannels to corporations using it to generate profit. The Costs of Connection uncovers this process, this "data colonialism," and its designs for controlling our lives—our ways of knowing; our means of production; our political participation. Colonialism might seem like a thing of the past, but this book shows that the historic appropriation of land, bodies, and natural resources is mirrored today in this new era of pervasive datafication. Apps, platforms, and smart objects capture and translate our lives into data, and then extract information that is fed into capitalist enterprises and sold back to us. The authors argue that this development foreshadows the creation of a new social order emerging globally—and it must be challenged. Confronting the alarming degree of surveillance already tolerated, they offer a stirring call to decolonize the internet and emancipate our desire for connection.
Digital Security in a Networked World Henry Holt and Company
Presenting invaluable advice from the world?s most famous computer security expert, this intensely readable collection features some of the most insightful and informative coverage of the strengths and weaknesses of computer security and the price people pay -- figuratively and literally -- when security fails. Discussing the issues surrounding things such as airplanes, passports, voting machines, ID cards, cameras, passwords, Internet banking, sporting events, computers, and castles, this book is a must-read for anyone who values security at any level -- business, technical, or personal.
Solving Cyber Risk Kogan Page Publishers
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.
Gray Day W. W. Norton & Company
The non-technical handbook for cyber security risk management Solving Cyber Risk distills a decade of research into a practical framework for cyber security. Blending statistical data and cost information with research into the culture, psychology, and business models of the hacker community, this book provides business executives, policy-makers, and individuals with a deeper understanding of existing future threats, and an action plan for safeguarding their organizations. Key Risk Indicators reveal vulnerabilities based on organization type, IT infrastructure and existing security measures, while expert discussion from leading cyber risk specialists details practical, real-world methods of risk reduction and mitigation. By the nature of the business, your organization's customer database is packed with highly sensitive information that is essentially hacker-bait, and even a minor flaw in security protocol could spell disaster. This book takes you deep into the cyber threat landscape to show you how to keep your data secure. Understand who is carrying out cyber-attacks, and why Identify your organization's risk of attack and vulnerability to damage Learn the most cost-effective risk reduction measures Adopt a new cyber risk assessment and quantification framework based on techniques used by the insurance industry By applying risk management principles to cyber security, non-technical leadership gains a greater understanding of the types of threat, level of threat, and level of investment needed to fortify the organization against attack. Just because you have not been hit does not mean your data is safe, and hackers rely on their targets' complacence to help maximize their haul. Solving Cyber Risk gives you a concrete action plan for implementing top-notch preventative measures before you're forced to implement damage control.