Ghost In The Wires My Adventures As The Worlds Most Wanted Hacker

Hacker extraordinaire Kevin Mitnick delivers the explosive encore to his bestselling The Art of Deception Kevin Mitnick, the world's most celebrated hacker, now devotes his life to helping businesses and governments combat data thieves, cybervandals, and other malicious computer intruders. In his bestselling The Art of Deception, Mitnick presented fictionalized case studies that illustrated how savvy computer crackers use "social engineering" to compromise even the most technically secure computer systems. Now, in his new book, Mitnick goes one step further, offering hair-raising stories of real-life computer break-ins-and showing how the victims could have prevented them. Mitnick's reputation within the hacker community gave him unique credibility with the perpetrators of these crimes, who freely shared their stories with him-and whose exploits Mitnick now reveals in detail for the first time, including: A group of friends who won nearly a million dollars in Las Vegas by reverse-engineering slot machines Two teenagers who were persuaded by terrorists to hack into the Lockheed Martin computer systems Two convicts who joined forces to become hackers inside a Texas prison A "Robin Hood" hacker who penetrated the computer systems of many prominent companies-andthen told them how he gained access With riveting "you are there" descriptions of real computer break-ins, indispensable tips on countermeasures security professionals need to implement now, and Mitnick's own acerbic commentary on the crimes he describes, this book is sure to reach a wide audience-and attract the attention of both law enforcement agencies and the media.

Real-world advice on how to be invisible online from "the FBI's most-wanted hacker" (Wired) Your every step online is being tracked and stored, and your identity easily stolen. Big companies and big governments want to know and exploit what you do, and privacy is a luxury few can afford or understand. In this explosive yet practical book, computer-security expert Kevin Mitnick uses true-life stories to show exactly what is happening without your knowledge, and teaches you "the art of invisibility": online and everyday tactics to protect you and your family, using easy step-by-step instructions. Reading this book, you will learn everything from password protection and smart Wi-Fi usage to advanced techniques designed to maximize your anonymity. Invisibility isn't just for superheroes--privacy is a power you deserve and need in the age of Big Brother and Big Data.

The first book to reveal and dissect the technical aspect of many social engineering maneuvers From elicitation, pretexting, influence and manipulation all aspects of social engineering are picked apart, discussed and explained by using real world examples, personal experience and the science behind them to unraveled the mystery in social engineering. Kevin Mitnick—one of the most famous social engineers in the world—popularized the term “social engineering.” He explained that it is much easier to trick someone into revealing a password for a system than to exert the effort of hacking into the system. Mitnick claims that this social engineering tactic was the single-most effective method in his arsenal. This indispensable book examines a variety of maneuvers that are aimed at deceiving unsuspecting victims, while it also addresses ways to prevent social engineering threats. Examines social engineering, the science of influencing a target to perform a desired task or divulge information Arms you with invaluable information about the many methods of trickery that hackers use in order to gather information with the intent of executing identity theft, fraud, or gaining computer system access Reveals vital steps for preventing social engineering threats Social Engineering: The Art of Human Hacking does its part to prepare you against nefarious hackers—now you can do your part by putting to good use the critical information within its pages.

A top cybersecurity journalist 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. “Immensely enjoyable . . . Zetter turns a complicated and technical cyber story into an engrossing whodunit.”—The Washington Post The virus now known as Stuxnet was unlike any other piece of malware built before: Rather than simply hijacking targeted computers or stealing information from them, it proved that a piece of code could escape the digital realm and wreak actual, physical destruction—in this case, on an Iranian nuclear facility. In these pages, journalist Kim Zetter tells the whole story behind the world’s first cyberweapon, covering its genesis in the corridors of the White House and its effects in Iran—and telling the spectacular, unlikely tale of the security geeks who managed to unravel a top secret sabotage campaign years in the making. But Countdown to Zero Day also ranges beyond Stuxnet itself, exploring the history of cyberwarfare and its future, showing us what might happen should our infrastructure be targeted by a Stuxnet-style attack, and ultimately, providing a portrait of a world at the edge of a new kind of war.

My Undercover Mission to Expose America's First Cyber Spy
How to Create Killer Blogs, Podcasts, Videos, Ebooks, Webinars (and More) That Engage Customers and Ignite Your Business
Hardware Hacking
America the Vulnerable
A Jeff Aiken Novel
Gray Hat Hacking, Second Edition
CUCKOO'S EGG

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.

Now available in a new edition entitled GLASS HOUSES: Privacy, Secrecy, and Cyber Insecurity in a Transparent World. A former top-level National Security Agency insider goes behind the headlines to explore America's next great battleground: digital security. An urgent wake-up call that identifies our foes; unveils their methods; and charts the dire consequences for government, business, and individuals. Shortly after 9/11, Joel Brenner entered the inner sanctum of American espionage, first as the inspector general of the National Security Agency, then as the head of counterintelligence for the director of national intelligence. He saw at close range the battleground on which our adversaries are now attacking us-cyberspace. We are at the mercy of a new generation of spies who operate remotely from China, the Middle East, Russia, even France, among many other places. These operatives have already shown their ability to penetrate our power plants, steal our latest submarine technology, rob our banks, and invade the Pentagon's secret communications systems. Incidents like the WikiLeaks posting of secret U.S. State Department cables hint at the urgency of this problem, but they hardly reveal its extent or its danger. Our government and corporations are a "glass house," all but transparent to our adversaries. Counterfeit computer chips have found their way into our fighter aircraft; the Chinese stole a new radar system that the navy spent billions to develop; our own soldiers used intentionally corrupted thumb drives to download classified intel from laptops in Iraq. And much more. Dispatches from the corporate world are just as dire. In 2008, hackers lifted customer files from the Royal Bank of Scotland and used them to withdraw $9 million in half an hour from ATMs in the United States, Britain, and Canada. If that was a traditional heist, it would be counted as one of the largest in history. Worldwide, corporations lose on average $5 million worth of intellectual property apiece annually, and big companies lose many times that. The structure and culture of the Internet favor spies over governments and corporations, and hackers over privacy, and we've done little to alter that balance. Brenner draws on his extraordinary background to show how to right this imbalance and bring to cyberspace the freedom, accountability, and security we expect elsewhere in our lives. In America the Vulnerable, Brenner offers a chilling and revelatory appraisal of the new faces of war and espionage-virtual battles with dangerous implications for government, business, and all of us.

Charles de Lint's Newford novels, loosely linked "tales" with overlapping characters set in an imaginary modern North American city, are tales of magic and myth afoot on today's city streets. But at the center of every de Lint story is the miracle of the human heart. And at the heart of Spirits in the Wires are Saskia Madding and Christiana Tree, both of whom are tied to perennial Newford character, the writer Christy Riddell. Are either Saskia or Christiana real? Christy's girlfriend, Saskia, believes she was born in a Web site, while Christiana is Christy's "shadow-self"--all the parts of him that he cast out when he was seven years old. At a popular Newford on-line research and library Web site called the Wordwood, a mysterious "crash" occurs. Everyone visiting the site at the moment of the crash vanishes from where they were sitting in front of their computers. Saskia disappears right before Christy's eyes, along with countless others. Now Christy and his companions must journey into Newford's otherworld, where the Wordwood, it transpires, has a physical presence of its own...to rescue their missing friends and loved ones and to set this viral spirit right before it causes further harm. At the Publisher's request, this title is being sold without Digital Rights Management Software (DRM) applied.

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

Social Engineering
Hacked Again
Trojan Horse
The Art of Invisibility
Alchemy of Bones
Cult of the Dead Cow
Physical Penetration Testing For IT Security Teams

The world's most famous former computer hacker, now a security consultant, describes his life on the run from the FBI creating fake identities, finding jobs at a law firm and a hospital and keeping tabs on his pursuers.

Former hacker Kevin Poulsen has, over the past decade, built a reputation as one of the top investigative reporters on the cybercrime beat. In Kingpin, he pours his unmatched access and expertise into book form for the first time, delivering a gripping cat-and-mouse narrative—and an unprecedented view into the twenty-first century’s signature form of organized crime. The word spread through the hacking underground like some unstoppable new virus: Someone—some brilliant, audacious crook—had just staged a hostile takeover of an online criminal network that siphoned billions of dollars from the US economy. The FBI rushed to launch an ambitious undercover operation aimed at tracking down this new kingpin; other agencies around the world deployed dozens of moles and double agents. Together, the cybercops lured numerous unsuspecting hackers into their clutches. . . . Yet at every turn, their main quarry displayed an uncanny ability to sniff out their snitches and see through their plots. The culprit they sought was the most unlikely of criminals: a brilliant programmer with a hippie ethic and a supervillain’s double identity. As prominent “white-hat” hacker Max “Vision” Butler, he was a celebrity throughout the programming world, even serving as a consultant to the FBI. But as the black-hat “Iceman,” he found in the world of data theft an irresistible opportunity to test his outsized abilities. He infiltrated thousands of computers around the country, sucking down millions of credit card numbers at will. He effortlessly hacked his fellow hackers, stealing their ill-gotten gains from under their noses. Together with a smooth-talking con artist, he ran a massive real-world crime ring. And for years, he did it all with seeming impunity, even as countless rivals ran afoul of police. Yet as he watched the fraudsters around him squabble, their ranks riddled with infiltrators, their methods inefficient, he began to see in their dysfunction the ultimate challenge: He would stage his coup and fix what was broken, run things as they should be run—even if it meant painting a bull’s-eye on his forehead. Through the story of this criminal’s remarkable rise, and of law enforcement’s quest to track him down, Kingpin lays bare the workings of a silent crime wave still affecting millions of Americans. In these pages, we are ushered into vast online-fraud supermarkets stocked with credit card numbers, counterfeit checks, hacked bank accounts, dead drops, and fake passports. We learn the workings of the numerous hacks—browser exploits, phishing attacks, Trojan horses, and much more—these fraudsters use to ply their trade, and trace the complex routes by which they turn stolen data into millions of dollars. And thanks to Poulsen’s remarkable access to both cops and criminals, we step inside the quiet, desperate arms race that law enforcement continues to fight with these scammers today. Ultimately, Kingpin is a journey into an underworld of startling scope and power, one in which ordinary American teenagers work hand in hand with murderous Russian mobsters and where a simple Wi-Fi connection can unleash a torrent of gold worth millions.

"A fantastic book for anyone looking to learn the tools and techniques needed to break in and stay in." --Bruce Potter, Founder, The Shmoo Group "Very highly recommended whether you are a seasoned professional or just starting out in the security business." --Simple Nomad, Hacker

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

The true story of Max Butler, the master hacker who ran a billion dollar cyber crime network
Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency
Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare
We Are Anonymous
Chicago's Luetgert Murder Case of 1897
Terry Pratchett: A Life With Footnotes
Hacks that Shocked the Business World

'Always readable, illuminating and honest. It made me miss the real Terry.' - NEIL GAIMAN 'Sometimes joyfully, sometimes painfully, intimate . . . it is wonderful to have this closeup picture of the writer's working life.' - FRANK COTTRELL-BOYCE, OBSERVER 'Spins magic from mundanity in precisely the way Pratchett himself did.' - THE TELEGRAPH 'As frank, funny and unsentimental as anything its subject might have produced himself.' - MAIL ON SUNDAY -------- At the time of his death in 2015, award-winning and bestselling author Sir Terry Pratchett was working on his finest story yet - his own. The creator of the phenomenally bestselling Discworld series, Terry Pratchett was known and loved around the world for his hugely popular books, his smart satirical humour and the humanity of his campaign work. But that's only part of the picture. Before his untimely death, Terry was writing a memoir: the story of a boy who aged six was told by his teacher that he would never amount to anything and spent the rest of his life proving him wrong. For Terry lived a life full of astonishing achievements: becoming one of the UK's bestselling and most beloved writers, winning the prestigious Carnegie Medal and being awarded a knighthood. Now, the book Terry sadly couldn't finish has been written by Rob Wilkins, his former assistant, friend and now head of the Pratchett literary estate. Drawing on his own extensive memories, along with those of the author's family, friends and colleagues, Rob unveils the full picture of Terry's life - from childhood to his astonishing writing career, and how he met and coped with what he called the 'Embuggerance' of Alzheimer's disease. A deeply moving and personal portrait of the extraordinary life of Sir Terry Pratchett, written with unparalleled insight and filled with funny anecdotes, this is the only official biography of one of our finest authors. 'Of all the dead authors in the world, Terry Pratchett is the most alive.' - JOHN LLOYD

Expert guidance on the art and science of driving secure behaviors Transformational Security Awareness empowers security leaders with the information and resources they need to assemble and deliver effective world-class security awareness programs that drive secure behaviors and culture change. When all other processes, controls, and technologies fail, humans are your last line of defense. But, how can you prepare them? Frustrated with ineffective training paradigms, most security leaders know that there must be a better way. A way that engages users, shapes behaviors, and fosters an organizational culture that encourages and reinforces security-related values. The good news is that there is hope. That’s what Transformational Security Awareness is all about. Author Perry Carpenter weaves together insights and best practices from experts in communication, persuasion, psychology, behavioral economics, organizational culture management, employee engagement, and storytelling to create a multidisciplinary masterpiece that transcends traditional security education and sets you on the path to make a lasting impact in your organization. Find out what you need to know about marketing, communication, behavior science, and culture management Overcome the knowledge-intention-behavior gap Optimize your program to work with the realities of human nature Use simulations, games, surveys, and leverage new trends like escape rooms to teach security awareness Put effective training together into a well-crafted campaign with ambassadors Understand the keys to sustained success and ongoing culture change Measure your success and establish continuous improvements Do you care more about what your employees know or what they do? It's time to transform the way we think about security awareness. If your organization is stuck in a security awareness rut, using the same ineffective strategies, materials, and information that might check a compliance box but still leaves your organization wide open to phishing, social engineering, and security-related employee mistakes and oversights, then you NEED this book.

Dart for Absolute Beginners enables individuals with no background in programming to create their own web apps while learning the fundamentals of software development in a cutting edge language. Easily digested chapters, while comprehensive enough to explore the whole domain, are aimed at both hobbyists and professionals alike. The reader will not only gain an insight into Dart, but also the technologies behind the web. A firm foundation is laid for further programming studies. Dart is a new, innovative language developed by Google which is poised to take the web by storm. For client side web app development, Dart has many advantages over JavaScript. These include but are not limited to: improved speed, enforcement of programmatic structure, and improved facilities for software reuse. Best of all, Dart is automatically converted to JavaScript so that it works with all web browsers. Dart is a fresh start, without the baggage of the last two decades of the web. Why start learning to program with yesterday’s technology? Teaches you the fundamentals of programming and the technologies behind the web. Utilizes the cutting edge, easy to learn, structured Dart programming language so that your first steps are pointed towards the future of web development. No prior knowledge is required to begin developing your own web apps.

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.

The Official Biography
Spirits in the Wires
Go Programming For Hackers and Pentesters
Black Hat Go

The Penetration Tester's Guide
The Extraordinary Story of a Hacker Called "Alien"

The true story of Max Butler, the master hacker who ran a billion dollar cyber crime network. The word spread through the hacking underground like some unstoppable new virus: an audacious crook had staged a hostile takeover of an online criminal network that siphoned billions of dollars from the US economy. The culprit was a brilliant programmer with a hippie ethic and a supervillain's double identity. Max 'Vision' Butler was a white-hat hacker and a celebrity throughout the programming world, even serving as a consultant to the FBI. But there was another side to Max. As the black-hat 'Iceman', he'd seen the fraudsters around him squabble, their ranks riddled with infiltrators, their methods inefficient, and in their dysfunction was the ultimate challenge: he would stage a coup and steal their ill-gotten gains from right under their noses. Through the story of Max Butler's remarkable rise, KINGPIN lays bare the workings of a silent crime wave affecting millions worldwide. It exposes vast online-fraud supermarkets stocked with credit card numbers, counterfeit cheques, hacked bank accounts and fake passports. Thanks to Kevin Poulsen's remarkable access to both cops and criminals, we step inside the quiet,desperate battle that law enforcement fights against these scammers. And learn that the boy next door may not be all he seems.

Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World (9781119643371) was previously published as Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World (9781793464187). While this version features a new cover design and introduction, the remaining content is the same as the prior release and should not be considered a new or updated product. Looking for real-world advice from leading cybersecurity experts? You've found your tribe. Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World is your guide to joining the ranks of hundreds of thousands of cybersecurity professionals around the world. Whether you’re just joining the industry, climbing the corporate ladder, or considering consulting, Tribe of Hackers offers the practical know-how, industry perspectives, and technical insight you need to succeed in the rapidly growing information security market. This unique guide includes inspiring interviews from 70 security experts, including Lesley Carhart, Ming Chow, Bruce Potter, Robert M. Lee, and Jayson E. Street. Get the scoop on the biggest cybersecurity myths and misconceptions about security Learn what qualities and credentials you need to advance in the cybersecurity field Uncover which life hacks are worth your while Understand how social media and the Internet of Things has changed cybersecurity Discover what it takes to make the move from the corporate world to your own cybersecurity venture Find your favorite hackers online and continue the conversation Tribe of Hackers is a must-have resource for security professionals who are looking to advance their careers, gain a fresh perspective, and get serious about cybersecurity with thought-provoking insights from the world’s most noteworthy hackers and influential security specialists.

It's two years after the Zero Day attacks, and cyber-security analyst Jeff Aiken is reaping the rewards for crippling Al-Qaida's assault on the computer infrastructure of the Western world. His company is flourishing, and his relationship with former government agent Daryl Haugen has intensified since she became a part of his team. But the West is under its greatest threat yet. A revolutionary, invisible trojan that alters data without leaving a trace---more sophisticated than any virus seen before---has been identified, roiling international politics. Jeff and Daryl are summoned to root it out and discover its source. As the trojan penetrates Western intelligence, and the terrifying truth about its creator is revealed, Jeff and Daryl find themselves in a desperate race to reverse it as the fate of both East and West hangs in the balance. A thrilling suspense story and a sober warning from one of the world's leading experts on cyber-security, Trojan Horse exposes the already widespread use of international cyber-espionage as a powerful and dangerous weapon, and the lengths to which one man will go to stop it.

In this "intriguing, insightful and extremely educational" novel, the world's most famous hacker teaches you easy cloaking and counter-measures for citizens and consumers in the age of Big Brother and Big Data (Frank W. Abagnale). Kevin Mitnick was the most elusive computer break-in artist in history. He accessed computers and networks at the world's biggest companies -- and no matter how fast the authorities were, Mitnick was faster, sprinting through phone switches, computer systems, and cellular networks. As the FBI's net finally began to tighten, Mitnick went on the run, engaging in an increasingly sophisticated game of hide-and-seek that escalated through false identities, a host of cities, and plenty of close shaves, to an ultimate showdown with the Feds, who would stop at nothing to bring him down. Ghost in the Wires is a thrilling true story of intrigue, suspense, and unbelievable escapes -- and a portrait of a visionary who forced the authorities to rethink the way they pursued him, and forced companies to rethink the way they protect their most sensitive information. "Mitnick manages to make breaking computer code sound as action-packed as robbing a bank." -- NPR

Breaking and Entering
Kingpin
The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw - By the Man Who Did It
The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data
Cybersecurity Advice from the Best Hackers in the World
Tribe of Hackers
How One Hacker Took Over the Billion-Dollar Cybercrime Underground

The sensational story behind one the first criminal investigations to use forensic analy

Like the best-selling Black Hat Python, Black Hat Go explores the darker side of the popular Go programming language. This collection of short scripts will help you test your systems, build and automate tools to fit your needs, and improve your offensive security skillset. Black Hat Go explores the darker side of Go, the popular programming language revered by hackers for its simplicity, efficiency, and reliability. It provides an arsenal of practical tactics from the perspective of security practitioners and hackers to help you test your systems, build and automate tools to fit your needs, and improve your offensive security skillset, all using the power of Go. You'll begin your journey with a basic overview of Go's syntax and philosophy and then start to explore examples that you can leverage for tool development, including common network protocols like HTTP, DNS, and SMB. You'll then dig into various tactics and problems that penetration testers encounter, addressing things like data pilfering, packet sniffing, and exploit development. You'll create dynamic, pluggable tools before diving into cryptography, attacking Microsoft Windows, and implementing steganography. You'll learn how to: • Make performant tools that can be used for your own security projects • Create usable tools that interact with remote APIs • Scrape arbitrary HTML data • Use Go's standard package, net/http, for building HTTP servers • Write your own DNS server and proxy • Use DNS tunneling to establish a C2 channel out of a restrictive network • Create a vulnerability fuzzer to discover an application's security weaknesses • Use plug-ins and extensions to future-proof productsBuild an RC2 symmetric-key brute-forcer • Implant data within a Portable Network Graphics (PNG) image. Are you ready to add to your arsenal of security tools? Then let's Go!

Ghost in the WiresMy Adventures as the World's Most Wanted HackerOrbit Books

*"If I had this book 10 years ago, the FBI would never have found me!" -- Kevin Mitnick This book has something for everyone---from the beginner hobbyist with no electronics or coding experience to the self-proclaimed "gadget geek." Take an ordinary piece of equipment and turn it into a personal work of art. Build upon an existing idea to create something better. Have fun while voiding your warranty! Some of the hardware hacks in this book include: * Don't toss your iPod away when the battery dies! Don't pay Apple the $99 to replace it! Install a new iPod battery yourself without Apple's "help" * An Apple a day! Modify a standard Apple USB Mouse into a glowing UFO Mouse or build a FireWire terabyte hard drive and custom case * Have you played Atari today? Create an arcade-style Atari 5200 paddle controller for your favorite retro videogames or transform the Atari 2600 joystick into one that can be used by left-handed players * Modern game systems, too! Hack your PlayStation 2 to boot code from the memory card or modify your PlayStation 2 for homebrew game development * Videophiles unite! Design, build, and configure your own Windows- or Linux-based Home Theater PC * Ride the airwaves! Modify a wireless PCMCIA NIC to include an external antenna connector or load Linux onto your Access Point * Stick it to The Man! Remove the proprietary barcode encoding from your CueCat and turn it into a regular barcode reader * Hack your Palm! Upgrade the available RAM on your Palm m505 from 8MB to 16MB · Includes hacks of today's most popular gaming systems like Xbox and PS/2. · Teaches readers to unlock the full entertainment potential of their desktop PC. · Frees iMac owners to enhance the features they love and get rid of the ones they hate.*

How the Original Hacking Supergroup Might Just Save the World
A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing
The Art of Deception
Hacking- The art Of Exploitation
Countdown to Zero Day
Content Rules
The Big Brother Game

The dramatic true story of the capture of the world's most wanted cyberthief by brilliant computer expert Tsutomu Shimomura, describes Kevin Mitnick's long computer crime spree, which involved millions of dollars in credit card numbers and corporate trade secrets. Reprint. NYT.

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.

An airliner's controls abruptly fail mid-flight over the Atlantic. An oil tanker runs aground in Japan when its navigational system suddenly stops dead. Hospitals everywhere have to abandon their computer databases when patients die after being administered incorrect dosages of their medicine. In the Midwest, a nuclear power plant nearly becomes the next Chernobyl when its cooling systems malfunction. At first, these random computer failures seem like unrelated events. But Jeff Aiken, a former government analyst who quit in disgust after witnessing the gross errors that led up to 9/11, thinks otherwise. Jeff fears a more serious attack targeting the United States computer infrastructure is already under way. And as other menacing computer malfunctions pop up around the world, some with deadly results, he realizes that there isn't much time if he hopes to prevent an international catastrophe. Written by a global authority on cyber security, Zero Day presents a chilling "what if" scenario that, in a world completely reliant on technology, is more than possible today---it's a cataclysmic disaster just waiting to happen.

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.

Unauthorised Access
Summary of Kevin Mitnick's Ghost in the Wires
Cyber Wars
Ghost in the Wires
Stuxnet and the Launch of the World's First Digital Weapon
Dart for Absolute Beginners
What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors

“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 guide to creating engaging web content and building a loyal following, revised and updated Blogs, YouTube, Facebook, Twitter, Google+, and other platforms are giving everyone a "voice," including organizations and their customers. So how do you create the stories, videos, and blog posts that cultivate fans, arouse passion for your products or services, and ignite your business? Content Rules equips you for online success as a one-stop source on the art and science of developing content that people care about. This coverage is interwoven with case studies of companies successfully spreading their ideas online—and using them to establish credibility and build a loyal customer base. Find an authentic "voice" and craft bold content that will resonate with prospects and buyers and encourage them to share it with others Leverage social media and social tools to get your content and ideas distributed as widely as possible Understand why you are generating content—getting to the meat of your message in practical, commonsense language, and defining the goals of your content strategy Write in a way that powerfully communicates your service, product, or message across various Web mediums Boost your online presence and engage with customers and prospects like never before with Content Rules.

This text introduces the spirit and theory of hacking as well as the science behind it all; it also provides some core techniques and tricks of hacking so you can think like a hacker, write your own hacks or thwart potential system attacks. .Tailgating Hackers and ninja both like wearing black, and they do share the ability to slip inside a building and blend with the shadows. .Shoulder Surfing If you like having a screen on your laptop so you can see what you're working on, don't read this chapter. .Physical Security Locks are serious business and lock technicians are true engineers, most backed with years of hands-on experience. But what happens when you take the age-old respected profession of the locksmith and sprinkle it with hacker ingenuity? .Social Engineering with Jack Wiles Jack has trained hundreds of federal agents, corporate attorneys, CEOs and internal auditors on computer crime and security-related topics. His unforgettable presentations are filled with three decades of personal "war stories" from the trenches of Information Security and Physical Security. .Google Hacking A hacker doesn't even need his own computer to do the necessary research.-

The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers
The Art of Intrusion
The Untold Story of the Teenagers and Outlaws who Hacked Ma Bell
Transformational Security Awareness
No Tech Hacking
Exploding the Phone
Have Fun while Voiding your Warranty

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.

Please note: This is a companion version & not the original book. Sample Book Insights: #1 I grew up as an only child. My mom had several boyfriends and husbands, and I was abused by one of them. I was good at sports as a kid, but I became interested in magic when I was ten and saw how people enjoyed being deceived. #2 I grew up as an only child. I was good at sports, but I became interested in magic when I was ten and saw how people enjoyed being deceived. I wanted to learn everything about how the phone system worked. #3 I was good at sports as a kid, but I became interested in magic when I was ten and saw how people enjoyed being deceived. I wanted to learn everything about how the phone system worked. #4 I was signed up at a Hebrew school in Sherman Oaks, but I got booted for goofing off. I spent my weekends at a bookstore in North Hollywood called the Survival Bookstore, soaking up the knowledge that would turn out to be invaluable two decades later when I was on the run.

Kevin Mitnick was the most elusive computer break-in artist in history. He accessed computers and networks at the world's biggest companies -- and however fast the authorities were, Mitnick was faster, sprinting through phone switches, computer systems, and cellular networks. He spent years skipping through cyberspace, always three steps ahead and labeled unstoppable. But for Kevin, hacking wasn't just about technological feats-it was an old fashioned confidence game that required guile and deception to trick the unwitting out of valuable information. Driven by a powerful urge to accomplish the impossible, Mitnick bypassed security systems and blazed into major organizations including Motorola, Sun Microsystems, and Pacific Bell. But as the FBI's net began to tighten, Kevin went on the run, engaging in an increasingly sophisticated cat and mouse game that led through false identities, a host of cities, plenty of close shaves, and an ultimate showdown with the Feds, who would stop at nothing to bring him down. Ghost in the Wires is a thrilling true story of intrigue, suspense, and unbelievable escape, and a portrait of a visionary whose creativity, skills, and persistence forced the authorities to rethink the way they pursued him, inspiring ripples that brought permanent changes in the way people and companies protect their most sensitive information. - Publisher.

Kevin Mitnick, the world's most wanted computer hacker, managed to hack into some of the country's most powerful - and seemingly impenetrable - agencies and companies. By conning employees into giving him private information and maneuvering through layers of security, he gained access to data that no one else could. The suspenseful heart of the book unfolds as Mitnick disappears on a three-year run from the FBI. He creates fake identities, finds jobs at a law firm and hospital, and keeps tabs on his myriad pursuers - all while continuing to hack into computer systems and phone company switches that were considered flawless. A modern, technology-driven adventure story, GHOST IN THE WIRES is a dramatic account of the joy of outsmarting security programs, the satisfaction of code-cracking, and the thrill of unbelievable escape.

Gray Day

A Novel of Myth and Magic - On the Streets and On the Net

Eh

My Adventures as the World's Most Wanted Hacker

The Science of Human Hacking

Metasploit

The Art of Human Hacking

The first guide to planning and performing a physical penetration test on your computer's security Most IT security teams concentrate on keeping networks and systems safe from attacks from the outside-but what if your attacker was on the inside? While nearly all IT teams perform a variety of network and application penetration testing procedures, an audit and test of the physical location has not been as prevalent. IT teams are now increasingly requesting physical penetration tests, but there is little available in terms of training. The goal of the test is to demonstrate any deficiencies in operating procedures concerning physical security. Featuring a Foreword written by world-renowned hacker Kevin D. Mitnick and lead author of The Art of Intrusion and The Art of Deception, this book is the first guide to planning and performing a physical penetration test. Inside, IT security expert Wil Allsopp guides you through the entire process from gathering intelligence, getting inside, dealing with threats, staying hidden (often in plain sight), and getting access to networks and data. Teaches IT security teams how to break into their own facility in order to defend against such attacks, which is often overlooked by IT security teams but is of critical importance Deals with intelligence gathering, such as getting access building blueprints and satellite imagery, hacking security cameras, planting bugs, and eavesdropping on security channels Includes safeguards for consultants paid to probe facilities unbeknown to staff Covers preparing the report and presenting it to management In order to defend data, you need to think like a thief-let Unauthorised Access show you how to get inside.

Hacked Again details the ins and outs of cybersecurity expert and CEO of a top wireless security tech firm Scott Schober, as he struggles to understand: the motives and mayhem behind his being hacked. As a small business owner, family man and tech pundit, Scott finds himself leading a compromised life. By day, he runs a successful security company and reports on the latest cyber breaches in the hopes of offering solace and security tips to millions of viewers. But by night, Scott begins to realize his worst fears are only a hack away as he falls prey to an invisible enemy. When a mysterious hacker begins to steal thousands from his bank account, go through his trash and rake over his social media identity; Scott stands to lose everything he worked so hard for. But his precarious situation only fortifies Scott's position as a cybersecurity expert and also as a harbinger for the fragile security we all cherish in this digital life. Amidst the backdrop of major breaches such as Target and Sony, Scott shares tips and best practices for all consumers concerning email scams, password protection and social media overload: Most importantly, Scott shares his own story of being hacked repeatedly and bow he has come to realize that the only thing as important as his own cybersecurity is that of his readers and viewers. Part cautionary tale and part cyber self-help guide, Hacked Again probes deep into the dark web for truths and surfaces to offer best practices and share stories from an expert who has lived as both an enforcer and a victim in the world of cybersecurity. Book jacket.

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.

A cybersecurity expert and former FBI "ghost" tells the thrilling story of how he helped take down notorious FBI mole Robert Hanssen, the first Russian cyber spy. Eric O'Neill was only twenty-six when he was tapped for the case of a lifetime: a one-on-one undercover investigation of the FBI's top target, a man suspected of spying for the Russians for nearly two decades, giving up nuclear secrets, compromising intelligence, and betraying US assets. With zero training in face-to-face investigation, Eric found himself in a windowless, high-security office in the newly formed Information Assurance Section, tasked officially with helping the FBI secure its outdated computer system against hackers and spies--and unofficially with collecting evidence against his new boss, Robert Hanssen, an exacting and rage-prone veteran agent with a disturbing fondness for handguns. In the months that follow, Eric's self-esteem and young marriage unravel under the pressure of life in Room 9930, and he questions the very purpose of his mission. But as Hanssen outmaneuvers an intelligence community struggling to keep up with the new reality of cybersecurity, he also teaches Eric the game of spycraft. Eric will just have to learn to outplay his teacher if he wants to win. A tension-packed stew of power, paranoia, and psychological manipulation, Gray Day is also a cautionary tale of how the United States allowed Russia to become dominant in cyberespionage--and how we might begin to catch up.

Zero Day

Takedown

Controlling the Human Element of Security