The Art Of Deception Controlling Human Element Security Kevin D Mitnick

When people should go to the books stores, search introduction by shop, shelf by shelf, it is truly problematic. This is why we provide the book compilations in this website. It will definitely ease you to look guide **The Art Of Deception Controlling Human Element Security Kevin D Mitnick** as you such as.

By searching the title, publisher, or authors of guide you essentially want, you can discover them rapidly. In the house, workplace, or perhaps in your method can be all best area within net connections. If you goal to download and install the The Art Of Deception Controlling Human Element Security Kevin D Mitnick, it is no question easy then, back currently we extend the link to buy and make bargains to download and install The Art Of Deception Controlling Human Element Security Kevin D Mitnick therefore simple!

No Tech Hacking Independently Published
Discover The Real Techniques To Persuade And Brainwash Anyone Mind control, also known as brainwashing, involves a unique selection of tools and techniques that will allow you to lead people in conversations and establish connections that have them genuinely wanting to do whatever you have asked them to do. In many instances, they will even do so thinking it was their idea to do so, and that you haven't planted the idea in their mind at all. When you'll become truly skilled at mind control, you will be able to have and do anything you want. Whether you want to get a sale on something, make a sale, get money, go on a date, get a raise or a promotion, get more slack from your boss, grow your business, or do virtually anything else that requires other people to cooperate with your desires, you will be able to do so with everything you learn in this book. In addition to learning the important skills and techniques required to brainwash others, you will also learn how to never get caught. You will learn everything you need to in order to be a master at mind control and genuinely create the life you desire without anyone ever knowing how you did it. "Mind control is a powerful skill you have to master if you don't want to be influenced and brainwashed" Remember, if this information is available to you, it is available to others as well! Knowing these techniques will prevent yourself from being brainwashed and will ensure that you are always doing exactly what you want to be doing, and that no one else is controlling your fate. This is all about putting you back in control of your own life. In this book you'll also find real life examples that will teach you how to apply the techniques learned in the most effective and clever way to get results. You'll learn: Proven Techniques of Persuasion, Manipulation and Deception How To Manipulate Others Without Never Getting Caught Working Strategies To Protect Yourself From Being Brainwashed All The Truth Behind Mind Control And Dark Psychology Mind Control Techniques Already Used in Society How To Stay In Control Of The Conversation Examples of Mind Control Techniques in Real Life If you want to change your life as you know it and start having the type of success that all of your idols rave about, then it is time to take back control. This book will give you every tool you need to do that. The only question is: are you ready for the life of your dreams? Get the life you've always dreamed of! Scroll up and select BUY NOW!

Introductory Guide to Discover How to Stop Being Manipulated, Avoid Mind Control, Covert Persuasion, Deception and Learn the Art of Reading People Profile Books
Robert Ludlum is the acknowledged master of suspense and international intrigue. For over thirty years, in over twenty international bestsellers, he has a set a standard that has never been equaled. Now, with the Prometheus Deception, he proves that he is at the very pinnacle of his craft. Nicholas Bryson spent years as a deep cover operative for the American secret intelligence group, the Directorate. After critical undercover mission went horribly wrong, Bryson was retired to a new identity. Years later, his closely held cover is cracked and Bryson learns that the Directorate was not what it claimed - that he was a pawn in a complex scheme against his own country's interests. Now, it has become increasingly clear that the shadowy Directorate is headed for some dangerous endgame - but no one knows precisely who they are and what they are planning. With Bryson their only possible asset, the director of the CIA recruits Bryson to find, reinfiltrate, and stop the Directorate. But after years on the sidelines, Bryson's field skills are rusty, his contacts unreliable, and his instincts suspect. With everything he thought he knew about his own life in question, Bryson is all alone in a wilderness of mirrors - unsure what is and isn't true and who, if anyone, he can trust - with the future of millions in the balance.

The Art of Deception Wiley
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 Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing Wiley
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.

Hands on Hacking Little, Brown
Learn to identify the social engineer by non-verbal behavior Unmasking the Social Engineer: The Human Element of Security focuses on combining the science of understanding non-verbal communications with the knowledge of how social engineers, scam artists and con men use these skills to build feelings of trust and rapport in their targets. The author helps readers understand how to identify and detect social engineers and scammers by analyzing their non-verbal behavior. Unmasking the Social Engineer shows how attacks work, explains nonverbal communications, and demonstrates with visuals the connection of non-verbal behavior to social engineering and scamming. Clearly combines both the practical and technical aspects of social engineering security Reveals the various dirty tricks that scammers use Pinpoints what to look for on the nonverbal side to detect the social engineer Sharing proven scientific methodology for reading, understanding, and deciphering non-verbal communications, Unmasking the Social Engineer arms readers with the knowledge needed to help protect their organizations.

The Art of Investigative Interviewing Syngress
An examination of one of the greatest success stories of the digital age looks at the success Steve Jobs has had with Pixar and his rejuvenation of Apple through the introduction of the iMac and iPod.

Cybersecurity Blue Team Toolkit John Wiley & Sons
The Art of Psychological Warfare, Human Hacking, Persuasion, and Deception Are You Ready To Learn How To Configure & Operate Cisco Equipment? If So You've Come To The Right Place - Regardless Of How Little Experience You May Have! If you're interested in social engineering and security then you're going to want (or need!) to know and understand the way of the social engineer. There's a ton of other guides out there that aren't clear and concise, and in my opinion use far too much jargon. My job is to teach you in simple, easy to follow terms how to understand social engineering. Here's A Preview Of What This Social Engineering Book Contains... What Is Social Engineering? Basic Psychological Tactics Social Engineering Tools Pickup Lines Of Social Engineers How To Prevent And Mitigate Social Engineering Attacks And Much, Much More! Order Your Copy Now And Learn All About Social Engineering!

ICon Steve Jobs John Wiley & Sons
The Art of Investigative Interviewing, Third Edition can be used by anyone who is involved in investigative interviewing. It is a perfect combination of real, practical, and effective techniques, procedures, and actual cases. Learn key elements of investigative interviewing, such as human psychology, proper interview preparation, tactical concepts, controlling the interview environment, and evaluating the evidence obtained from the interview. Inge Sebyan Black updated the well-respected work of Charles L. Yeschke to provide everything an interviewer needs to know in order to conduct successful interviews professionally, with integrity, and within the law. This book covers the myriad factors of an interview — including issues of evidence, rapport, deception, authority, and setting — clearly and effectively. It also includes a chapter on personnel issues and internal theft controls. Provides guidance on conducting investigative interviews professionally and ethically Includes instructions for obtaining voluntary confessions from suspects, victims, and witnesses Builds a foundation of effective interviewing skills with guidance on every step of the process, from preparation to evaluating evidence obtained in an interview

Outwitting the Devil Broadway Books
"I speak the truth, not so much as I would, but as much as I dare...."-- Montaigne "All cruel people describe themselves as paragons of frankness.'" -- Tennessee Williams Truth and deception--like good and evil--have long been viewed as diametrically opposed and unreconcilable. Yet, few people can honestly claim they never lie. In fact, deception is practiced habitually in day-to-day life--from the polite compliment that doesn't accurately relay one's true feelings, to self-deception about one's own motivations. What fuels the need for people to intricately construct lies and illusions about their own lives? If deceptions are unconscious, does it mean that we are not responsible for their consequences? Why does self-deception or the need for illusion make us feel uncomfortable? Taking into account the sheer ubiquity and ordinariness of deception, this interdisciplinary work moves away from the cut-and-dried notion of duplicity as evil and illuminates the ways in which deception can also be understood as a adaptive response to the demands of living with others. The book articulates the boundaries between unethical and adaptive deception demonstrating how some lies serve socially approved goals, while others provoke distrust and condemnation. Throughout, the volume focuses on the range of emotions--from feelings of shame, fear, or envy, to those of concern and compassion--that motivate our desire to deceive ourselves and others. Providing an interdisciplinary exploration of the widespread phenomenon of lying and deception, this volume promotes a more fully integrated understanding of how people function in their everyday lives. Case illustrations, humor and wit, concrete examples, and even a mock television sitcom script bring the ideas to life for clinical practitioners, behavioral scientists, and philosophers, and for students in these realms.

Protect to Enable Diana Brain
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.

Kingpin Cambridge University Press
In this "intriguing, insightful and extremely educational" novel, the world's most famous hacker teaches you easy cloaking and counter-measures for citizens and consumers in the age of Big Brother and Big Data (Frank W. Abagnale). Kevin Mitnick was the most elusive computer break-in artist in history. He accessed computers and networks at the world's biggest companies -- and no matter how fast the authorities were, Mitnick was faster, sprinting through phone switches, computer systems, and cellular networks. As the FBI's net finally began to tighten, Mitnick went on the run, engaging in an increasingly sophisticated game of hide-and-seek that escalated

through false identities, a host of cities, and plenty of close shaves, to an ultimate showdown with the Feds, who would stop at nothing to bring him down. Ghost in the Wires is a thrilling true story of intrigue, suspense, and unbelievable escapes -- and a portrait of a visionary who forced the authorities to rethink the way they pursued him, and forced companies to rethink the way they protect their most sensitive information. "Mitnick manages to make breaking computer code sound as action-packed as robbing a bank." -- NPR

The Kiss of Deception Profile Books

Documents how a troubled young computer hacker seized control of a massive international computer fraud network in 2006, tracing the efforts of FBI and Secret Service agents as well as an undercover operator to locate and arrest him. Reprint.

Controlling the Human Element of Security Butterworth-Heinemann

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.

Sharon Lechter

"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.

Human Hacking Prometheus Books

Take on the perspective of an attacker with this insightful new resource for ethical hackers, pentesters, and social engineers In The Art of Attack: Attacker Mindset for Security Professionals, experienced physical pentester and social engineer Maxie Reynolds untangles the threads of a useful, sometimes dangerous, mentality. The book shows ethical hackers, social engineers, and pentesters what an attacker mindset is and how to use it to their advantage. Adopting this mindset will result in the improvement of security, offensively and defensively, by allowing you to see your environment objectively through the eyes of an attacker. The book shows you the laws of the mindset and the techniques attackers use, from persistence to “start with the end” strategies and non-linear thinking, that make them so dangerous. You’ll discover: A variety of attacker strategies, including approaches, processes, reconnaissance, privilege escalation, redundant access, and escape techniques The unique tells and signs of an attack and how to avoid becoming a victim of one What the science of psychology tells us about amygdala hijacking and other tendencies that you need to protect against Perfect for red teams, social engineers, pentesters, and ethical hackers seeking to fortify and harden their systems and the systems of their clients, The Art of Attack is an invaluable resource for anyone in the technology security space seeking a one-stop resource that puts them in the mind of an attacker.

The Psychology of Online Offenders Rowman & Littlefield

Managing Risk and Information Security: Protect to Enable, an ApressOpen title, describes the changing risk environment and why a fresh approach to information security is needed. Because almost every aspect of an enterprise is now dependent on technology, the focus of IT security must shift from locking down assets to enabling the business while managing and surviving risk. This compact book discusses business risk from a broader perspective, including privacy and regulatory considerations. It describes the increasing number of threats and vulnerabilities, but also offers strategies for developing solutions. These include discussions of how enterprises can take advantage of new and emerging technologies—such as social media and the huge proliferation of Internet-enabled devices—while minimizing risk. With ApressOpen, content is freely available through multiple online distribution channels and electronic formats with the goal of disseminating professionally edited and technically reviewed content to the worldwide community. Here are some of the responses from reviewers of this exceptional work: “Managing Risk and Information Security is a perceptive, balanced, and often thought-provoking exploration of evolving information risk and security challenges within a business context. Harkins clearly connects the needed, but often-overlooked linkage and dialog between the business and technical worlds and offers actionable strategies. The book contains eye-opening security insights that are easily understood, even by the curious layman.” Fred Wettling, Bechtel Fellow, IS&T Ethics & Compliance Officer, Bechtel “As disruptive technology innovations and escalating cyber threats continue to create enormous information security challenges, Managing Risk and Information Security: Protect to Enable provides a much-needed perspective. This book compels information security professionals to think differently about concepts of risk management in order to be more effective. The specific and practical guidance offers a fast-track formula for developing information security strategies which are lock-step with business priorities.” Laura Robinson, Principal, Robinson Insight Chair, Security for Business Innovation Council (SBIC) Program Director, Executive Security Action Forum (ESAF) “The mandate of the information security function is being completely rewritten. Unfortunately most heads of security haven’t picked up on the change, impeding their companies’ agility and ability to innovate. This book makes the case for why security needs to change, and shows how to get started. It will be regarded as marking the turning point in information security for years to come.” Dr. Jeremy Bergsman, Practice Manager, CEB “The world we are responsible to protect is changing dramatically and at an accelerating pace. Technology is pervasive in virtually every aspect of our lives. Clouds, virtualization and mobile are redefining computing – and they are just the beginning of what is to come. Your security perimeter is defined by wherever your information and people happen to be. We are attacked by professional adversaries who are better funded than we will ever be. We in the information security profession must change as dramatically as the environment we protect. We need new skills and new strategies to do our jobs effectively. We literally need to change the way we think. Written by one of the best in the business, Managing Risk and Information Security challenges traditional security theory with clear examples of the need for change. It also provides expert advice on how to dramatically increase the success of your security strategy and methods – from dealing with the misperception of risk to how to become a Z-shaped CISO. Managing Risk and Information Security is the ultimate treatise on how to deliver effective security to the world we live in for the next 10 years. It is absolute must reading for anyone in our profession – and should be on the desk of every CISO in the world.” Dave Cullinane, CISSP CEO Security Starfish, LLC “In this overview, Malcolm Harkins delivers an insightful survey of the trends, threats, and tactics shaping information risk and security. From regulatory compliance to psychology to the changing threat context, this work provides a compelling introduction to an important topic and trains helpful attention on the effects of changing technology and management practices.” Dr. Mariano-Florentino Cuéllar Professor, Stanford Law School Co-Director, Stanford Center for International Security and Cooperation (CISAC), Stanford University “Malcolm Harkins gets it. In his new book Malcolm outlines the major forces changing the information security risk landscape from a big picture perspective, and then goes on to offer effective methods of managing that risk from a practitioner's viewpoint. The combination makes this book unique and a must read for anyone interested in IT risk." Dennis Devlin AVP, Information Security and Compliance, The George Washington University “Managing Risk and Information Security is the first-to-read, must-read book on information security for C-Suite executives. It is accessible, understandable and actionable. No sky-is-falling scare tactics, no techno-babble – just straight talk about a critically important subject. There is no better primer on the economics, ergonomics and psycho-behaviourals of security than this.” Thornton May, Futurist, Executive Director & Dean, IT Leadership Academy “Managing Risk and Information Security is a wake-up call for information security executives and a ray of light for business leaders. It equips organizations with the knowledge required to transform their security programs from a “culture of no” to one focused on agility, value and competitiveness. Unlike other publications, Malcolm provides clear and immediately applicable solutions to optimally balance the frequently opposing needs of risk reduction and business growth. This book should be required reading for anyone currently serving in, or seeking to achieve, the role of Chief Information Security Officer.” Jamil Farshchi, Senior Business Leader of Strategic Planning and Initiatives, VISA “For too many years, business and security – either real or imagined – were at odds. In Managing Risk and Information Security: Protect to Enable, you get what you expect – real life practical ways to break logjams, have security actually enable business, and marries security architecture and business architecture. Why this book? It's written by a practitioner, and not just any practitioner, one of the leading minds in Security today.” John Stewart, Chief Security Officer, Cisco “This book is an invaluable guide to help security professionals address risk in new ways in this alarmingly fast changing environment. Packed with examples which makes it a pleasure to read, the book captures practical ways a forward thinking CISO can turn information security into a competitive advantage for their business. This book provides a new framework for managing risk in an entertaining and thought provoking way. This will change the way security professionals work with their business leaders, and help get products to market faster. The 6 irrefutable laws of information security should be on a stone plaque on the desk of every security professional.” Steven Proctor, VP, Audit & Risk Management, Flextronics

A Novel John Wiley & Sons

Johnny Long's last book sold 12,000 units worldwide. Kevin Mitnick's last book sold 40,000 units in North America. As the cliché goes, information is power. In this age of technology, an increasing majority of the world's information is stored electronically. It makes sense then that we rely on high-tech electronic protection systems to guard that information. As professional hackers, Johnny Long and Kevin Mitnick get paid to uncover weaknesses in those systems and exploit them. Whether breaking into buildings or slipping past industrial-grade firewalls, their goal has always been the same: extract the information using any means necessary. After hundreds of jobs, they have discovered the secrets to bypassing every conceivable high-tech security system. This book reveals those secrets; as the title suggests, it has nothing to do with high technology. • Dumpster Diving Be a good sport and don’t read the two “D” words written in big bold letters above, and act surprised when I tell you hackers can accomplish this without relying on a single bit of technology (punny). • 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. If he can make it to a public library, Kinko's or Internet cafe, he can use Google to process all that data into something useful. • P2P Hacking Let’s assume a guy has no budget, no commercial hacking software, no support from organized crime and no fancy gear. With all those restrictions, is this guy still a threat to you? Have a look at this chapter and judge for yourself. • People Watching Skilled people watchers can learn a whole lot in just a few quick glances. In this chapter we’ll take a look at a few examples of the types of things that draws a no-tech hacker’s eye. • Kiosks What happens when a kiosk is more than a kiosk? What happens when the kiosk holds airline passenger information? What if the kiosk holds confidential patient information? What if the kiosk holds cash? • Vehicle Surveillance Most people don’t realize that some of the most thrilling vehicular espionage happens when the cars aren't moving at all!

Lying and Deception in Everyday Life St. Martin's Press

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

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

The Prometheus Deception John Wiley & Sons

The Art of War is an enduring classic that holds a special place in the culture and history of East Asia. An ancient Chinese text on the philosophy and politics of warfare and military strategy, the treatise was written in 6th century B.C. by a warrior-philosopher now famous all over the world as Sun Tzu. Sun Tzu's teachings remain as relevant to leaders and strategists today as they were to rulers and military generals in ancient times. Divided into thirteen chapters and written succinctly, The Art of War is a must-read for anybody who works in a competitive environment.

Have Fun while Voiding your Warranty Elsevier

Which sort of seducer could you be? Siren? Rake? Cold Coquette? Star? Comedian? Charismatic? Or Saint? This book will show you which. Charm, persuasion, the ability to create illusions: these are some of the many dazzling gifts of the Seducer, the compelling figure who is able to manipulate, mislead and give pleasure all at once. When raised to the level of art, seduction, an indirect and subtle form of power, has toppled empires, won elections and enslaved great minds. In this beautiful, sensually designed book, Greene unearths the two sides of seduction: the characters and the process. Discover who you, or your pursuer, most resembles. Learn, too, the pitfalls of the anti-Seducer. Immerse yourself in the twenty-four manoeuvres and strategies of the seductive process, the ritual by which a seducer gains mastery over their target. Understand how to 'Choose the Right Victim', 'Appear to Be an Object of Desire' and 'Confuse Desire and Reality'. In addition, Greene provides instruction on how to identify victims by type. Each fascinating character and each cunning tactic demonstrates a fundamental truth about who we are, and the targets we've become - or hope to win over. The Art of Seduction is an indispensable primer on the essence of one of history's greatest weapons and the ultimate power trip. From the internationally bestselling author of The 48 Laws of Power, Mastery, and The 33 Strategies Of War.