Practical Examples Of Social Engineering

When people should go to the book stores, search commencement by shop, shelf by shelf, it is really problematic. This is why we allow the book compilations in this website. It will definitely ease you to look guide **Practical Examples Of Social Engineering** as you such as.

By searching the title, publisher, or authors of guide you in point of fact want, you can discover them rapidly. In the house, workplace, or perhaps in your method can be all best place within net connections. If you set sights on to download and install the Practical Examples Of Social Engineering, it is very easy then, past currently we extend the connect to buy and create bargains to download and install Practical Examples Of Social Engineering suitably simple!

Kali Linux 2 – Assuring Security by Penetration Testing Routledge
Ian Mann's Hacking the Human highlights the main sources of risk from social engineering and draws on psychological models to explain the basis for human vulnerabilities. Offering more than a simple checklist to follow, the book provides a rich mix of examples, applied research and practical solutions for security and IT professionals that enable you to create and develop a security solution that is most appropriate for your organization.

Kali Linux Social Engineering Social Engineering
Social engineering attacks target the weakest link in an organization's security human beings. Everyone knows these attacks are effective, and everyone knows they are on the rise. Now, Social Engineering Penetration Testing gives you the practical methodology and everything you need to plan and execute a social engineering penetration test and assessment. You will gain fascinating insights into how social engineering techniques including email phishing, telephone pretexting, and physical vectors can be used to elicit information or manipulate individuals into performing actions that may aid in an attack. Using the book's easy-to-understand models and examples, you will have a much better understanding of how best to defend against these attacks. The authors of Social Engineering Penetration Testing show you hands-on techniques they have used at RandomStorm to provide clients with valuable results that make a real difference to the security of their businesses. You will learn about the differences between social engineering pen tests lasting anywhere from a few days to several months. The book shows you how to use widely available open-source tools to conduct your pen tests, then walks you through the practical steps to improve defense measures in response to test results. Understand how to plan and execute an effective social engineering assessment Learn how to configure and use the open-source tools available for the social engineer Identify parts of an assessment that will most benefit time-critical engagements Learn how to design target scenarios, create plausible attack situations, and support various attack vectors with technology Create an assessment report, then improve defense measures in response to test results

Wireless and Mobile Device Security Syngress
CompTIA® Security+ SY0-301 Practice Questions Exam Cram, Third Edition, offers all the exam practice you'll need to systematically prepare, identify and fix areas of weakness, and pass your exam the first time. This book complements any Security+ study plan with more than 800 practice test questions–all supported with complete explanations of every correct and incorrect answer–covering all Security+ exam objectives, including network security; compliance and operation security; threats and vulnerabilities; application, host and data security; access control and identity management; and cryptography. This is the eBook version of the print title. Note that the eBook does not provide access to the CD-ROM content that accompanies the print book. Limited Time Offer: Buy CompTIA Security+ SY0-301 Practice Questions Exam Cram and receive a 10% off discount code for the CompTIA Security+ SYO-301 exam. To receive your 10% off discount code: 1. Register your product at pearsonITcertification.com/register 2. When prompted, enter ISBN: 9780789748287 3. Go to your Account page and click on "Access Bonus Content" Covers the critical information you'll need to know to score higher on your Security+ exam! Features more than 800 questions that are organized according to the Security+ exam objectives, so you can easily assess your knowledge of each topic. Use our innovative Quick-Check Answer System™ to quickly find answers as you work your way through the questions. Each question includes detailed explanations! Our popular Cram Sheet, which includes tips, acronyms, and memory joggers, helps you review key facts before you enter the testing center. Diane M. Barrett (MCSE, CISSP, Security+) is the director of training for Paraben Corporation and an adjunct professor for American Military University. She has done contract forensic and security assessment work for several years and has authored other security and forensic books. She is a regular committee member for ADFSL's Conference on Digital Forensics, Security and Law, as well as an academy director for Advancement Solutions. She holds many industry certifications, including CISSP, ISSMP, DFCP, PCME, and Security+. Diane's education includes a MS in Information Technology with a specialization in Information Security. She expects to complete a PhD in business administration with a specialization in Information Security shortly.

The Social Engineer Virago
The best defense against the increasing threat of social engineering attacks is Security Awareness Training to warn your organization's staff of the risk and educate them on how to protect your organization's data. Social engineering is not a new tactic, but Building an Security Awareness Program is the first book that shows you how to build a successful security awareness training program from the ground up. Building an Security Awareness Program provides you with a sound technical basis for developing a new training program. The book also tells you the best ways to garner management support for implementing the program. Author Bill Gardner is one of the founding members of the Security Awareness Training Framework. Here, he walks you through the process of developing an engaging and successful training program for your organization that will help you and your staff defend your systems, networks, mobile devices, and data. Forewords written by Dave Kennedy and Kevin Mitnick! The most practical guide to setting up a Security Awareness training program in your organization Real world examples show you how cyber criminals commit their crimes, and what you can do to keep you and your data safe Learn how to propose a new program to management, and what the benefits are to staff and your company Find out about various types of training, the best training cycle to use, metrics for success, and methods for building an engaging and successful program

Techno Security's Guide to Managing Risks for IT Managers, Auditors, and Investigators MIT Press
Seven Deadliest USB Attacks provides a comprehensive view of the most serious types of Universal Serial Bus (USB) attacks. While the book focuses on Windows systems, Mac, Linux, and UNIX systems are equally susceptible to similar attacks. If you need to keep up with the latest hacks, attacks, and exploits effecting USB technology, then this book

is for you. This book pinpoints the most dangerous hacks and exploits specific to USB, laying out the anatomy of these attacks including how to make your system more secure. You will discover the best ways to defend against these vicious hacks with step-by-step instruction and learn techniques to make your computer and network impenetrable. The attacks outlined in this book are intended for individuals with moderate Microsoft Windows proficiency. The book provides the tools, tricks, and detailed instructions necessary to reconstruct and mitigate these activities while peering into the risks and future aspects surrounding the respective technologies. There are seven chapters that cover the following: USB Hacksaw; the USB Switchblade; viruses and malicious codes; USB-based heap overflow; the evolution of forensics in computer security; pod slurping; and the human element of security, including the risks, rewards, and controversy surrounding social-engineering engagements. This book was written to target a vast audience including students, technical staff, business leaders, or anyone seeking to understand fully the removable-media risk for Windows systems. It will be a valuable resource for information security professionals of all levels, as well as web application developers and recreational hackers. Knowledge is power, find out about the most dominant attacks currently waging war on computers and networks globally Discover the best ways to defend against these vicious attacks; step-by-step instruction shows you how Institute countermeasures, don ’ t be caught defenseless again, and learn techniques to make your computer and network impenetrable

Social Engineering John Wiley & Sons

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.

Behind Closed Doors: SHORTLISTED FOR THE ORWELL PRIZE FOR POLITICAL WRITING John Wiley & Sons

When it comes to network security, many users and administrators are running scared, and justifiably so. The sophistication of attacks against computer systems increases with each new Internet worm.What's the worst an attacker can do to you? You'd better find out, right? That's what Security Warrior teaches you. Based on the principle that the only way to defend yourself is to understand your attacker in depth, Security Warrior reveals how your systems can be attacked. Covering everything from reverse engineering to SQL attacks, and including topics like social engineering, antiforensics, and common attacks against UNIX and Windows systems, this book teaches you to know your enemy and how to be prepared to do battle.Security Warrior places particular emphasis on reverse engineering. RE is a fundamental skill for the administrator, who must be aware of all kinds of malware that can be installed on his machines -- trojaned binaries, "spyware" that looks innocuous but that sends private data back to its creator, and more. This is the only book to discuss reverse engineering for Linux or Windows CE. It's also the only book that shows you how SQL injection works, enabling you to inspect your database and web applications for vulnerability.Security Warrior is the most comprehensive and up-to-date book covering the art of computer war: attacks against computer systems and their defenses. It's often scary, and never comforting. If you're on the front lines, defending your site against attackers, you need this book. On your shelf--and in your hands.

Encyclopedia of Business Ethics and Society Hachette UK

Improve information security by learning Social Engineering. Key Features Learn to implement information security using social engineering Get hands-on experience of using different tools such as Kali Linux, the Social Engineering toolkit and so on Practical approach towards learning social engineering, for IT security Book Description This book will provide you with a holistic understanding of social engineering. It will help you to avoid and combat social engineering attacks by giving you a detailed insight into how a social engineer operates. Learn Social Engineering starts by giving you a grounding in the different types of social engineering attacks,and the damages they cause. It then sets up the lab environment to use different toolS and then perform social engineering steps such as information gathering. The book covers topics from baiting, phishing, and spear phishing, to pretexting and scareware. By the end of the book, you will be in a position to protect yourself and your systems from social engineering threats and attacks. All in all, the book covers social engineering from A to Z , along with excerpts from many world wide known security experts. What you will learn Learn to implement information security using social engineering Learn social engineering for IT security Understand the role of social media in social engineering Get acquainted with Practical Human hacking skills Learn to think like a social engineer Learn to beat a social engineer Who this book is for This book targets security professionals, security analysts, penetration testers, or any stakeholder working with information security who wants to learn how to use social engineering techniques. Prior knowledge of Kali Linux is an added advantage

Human Hacking Routledge

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.

Elsevier

"Nina Schick is alerting us to a danger from the future that is already here." - Adam Boulton, Editor at Large, Sky News "Deep Fakes and the Infocalypse is an urgent, thoughtful and thoroughly-researched book that raises uncomfortable questions about the way that information is being distorted by states and individuals... A must-read." - Greg Williams, Editor in Chief of WIRED UK "Essential reading for any one interested about the shocking way information is and will be manipulated." - Lord Edward Vaizey "Schick's Deep Fakes and the Infocalypse is a short, sharp book that hits you like a punch in the stomach." - Nick Cohen, The Observer "Deep Fakes is an uncomfortable but gripping read, probing the way in which the internet has been flooded with disinformation and dark arts propaganda." - Jim Pickard, Chief Political Correspondent, Financial Times "A searing insight into a world so many of us find difficult to understand. I was gripped from the first page." - Iain Dale, Broadcaster "With this powerful book, Nina Schick has done us all a great public service...It's your civic duty to read it." - Jamie Susskind, author of Future Politics "Gripping, alarming and morally vital." - Ian Dunt, Host of Remainiacs Podcast Deep Fakes are coming, and we are not ready. Advanced AI technology is now able to create video of people doing things they never did, in places they have never been, saying things they never said. In the hands of rogue states, terrorists, criminals or crazed individuals, they represent a disturbing new threat to democracy and personal liberty. Deep Fakes can be misused to shift public opinion, swing Presidential elections, or blackmail, coerce, and silence individuals. And when combined with the destabilising overload of disinformation that has been dubbed 'the Infocalypse', we are potentially facing a danger of world-changing proportions. Deep Fakes and the Infocalypse is International Political Technology Advisor Nina Schick's stark warning about a future we all need to understand before it's too late.

CompTIA Security+ SY0-201 Practice Questions Exam Cram John Wiley & Sons

Over the last several decades, questions about practical reason have come to occupy the center stage in ethics and metaethics. The Routledge Handbook of Practical Reason is an outstanding reference source to this exciting and distinctive subject area and is the first volume of its kind. Comprising thirty-six chapters by an international team of contributors, the Handbook provides a comprehensive overview of the field and is divided into five parts: Foundational Matters Practical Reason in the History of Philosophy Philosophy of Practical Reason as Action Theory and Moral Psychology Philosophy of Practical Reason as Theory of Practical Normativity The Philosophy of Practical Reason as the Theory of Practical Rationality The Handbook also includes two chapters by the late Derek Parfit, ‘ Objectivism about Reasons ’ and ‘ Normative Non-Naturalism. ’ The Routledge Handbook of Practical Reason is essential reading for philosophy students and researchers in metaethics, philosophy of action, action theory, ethics, and the history of philosophy.

Hacking McGill-Queen's Press - MQUP

'BRILLIANT . . . I LOVE THIS BOOK' LEMN SISSAY 'A MUST-READ BOOK' JACQUELINE WILSON 'EXTRAORDINARY' OLIVER BULLOUGH 'EVERYONE SHOULD READ THIS BOOK' HILARY COTTAM Meet the mother whose children were taken away, and the father who fought for his son. Listen to the radical social worker, the judge, the lawyer. See inside the homes of foster carers, adoptive parents and children in care. Because behind closed doors, a scandal is ongoing. We now remove more children from their parents than ever before, more than any other western country. Not because of a rise in physical or sexual abuse, but because of complex factors that are overlooked and misunderstood. Children's Care is a system where fathers are ignored, and mothers are punished for experiencing abuse. Rife with prejudices about race, ableism and class, determined by a postcode lottery. Blind to poverty and its effects on family life. And, at its very worst, an exercise in social engineering that can never replace parental love. This is not a soft issue. Not a 'women and children' problem. It is a prism through which we can understand the deepest issues at play in politics, economics and society today, and it is happening behind closed doors. Because of legal restrictions against reporting in family courts, the uneasy work of social care and the shame poured on parents, these problems remain out of our sight. They are the subject of horror headlines or stale statistics. But family life is at the heart of who we are as people, and it is they who can help us understand. From North to South, rich and poor, Black and white, these are the people who know, first-hand, what is going wrong - and how we can fix it. These are their stories. 'IMPORTANT' IAN BIRRELL 'VITAL' HANNAH JANE PARKINSON 'ONE OF BRITAIN'S BEST JOURNALISTS WRITING ABOUT SOCIAL JUSTICE' MARIANA MAZZUCATO

Social Policy: An Introduction McGraw-Hill Education (UK)

Macro-social marketing is an approach to solving wicked problems. Wicked problems include obesity, environmental degradation, smoking cessation, fast fashion, gambling, and drug and alcohol abuse. As such, wicked problems are those problems that are so complex and multifaceted, it is difficult to define the exact problem, its contributing factors, and paths to a solution. Increasingly, governments, NGOs, and community groups are seeking to solve these types of problems. In doing so, the issues with pursuing macro-level change are beginning to emerge. Issues stem from the interconnected nature of stakeholders involved with a wicked problem—where one change may create a negative ripple effect of both intended and unintended consequences. Macro-social marketing, then, provides a holistic and systemic approach to both studying and solving wicked problems. Within the chapters of this book, macro-social marketing approaches to analysing and defining wicked problems, to identifying stakeholders and potential ripple effects, and to implementing macro-level change are presented. In this emerging area of academia, the theories, models, and approaches outlined in this book are cutting edge and provide a critical approach from top researchers in the area. Both practical and theoretical aspects are presented as well as caveats on such societal and/or country-wide change. A must-have for social marketing academics and those interested in macro-level change at a practical or theoretical level.

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

Philosophical Foundations of the Three Sociologies (RLE Social Theory) Jones & Bartlett Learning
In order to understand hackers and protect the network infrastructure you must think like a hacker in today's expansive and eclectic internet and you must understand that nothing is fully secured.This book will focus on social engineering techniques that are favourite of both, White Hat and Black Hat hackers.If you attempt to use any of the tools or techniques discussed in this book on a network without being authorized and you disturb or damage any systems, that would be considered illegal black hat hacking. So, I would like to encourage all readers to deploy any tool and method described in this book for WHITE HAT USE ONLY.The focus of this book will be to introduce some of the most well known social engineering techniques.This book contains step by step deployment guides of performances on how to plan a successful penetration test and examples on how to manipulate or misdirect trusted employees using social engineering.Your reading of this book will boost your knowledge on what is possible in today's hacking world and help you to become an Ethical Hacker aka Penetration Tester.BUY THIS BOOK NOW AND GET STARTED TODAY!IN THIS BOOK YOU WILL LEARN ABOUT: -Phishing, Vishing, Smishing, Spear Phishing and Whaling-The history of social engineering-Psychological manipulation-Human Weaknesses-Social Engineering Categories-Cold Call Virus Scams-Authority & Fear Establishment-Executing the Social Engineering Attack-Signifying Legitimacy by Providing Value-Open-Source Intelligence-Organizational Reconnaissance-Identifying Targets Within an Organization-In-person social engineering techniques-Dumpster Diving & Data Breaches-Phishing Page Types-Filter Evasion Techniques-How to use PhishTank and Phish5-Identity Theft and Impersonation-Social Engineering Countermeasures-Paper & Digital Record Destruction-Physical Security Measures-Principle of Least Privilege-2FA & Side Channel ID Verification-Logging & Monitoring-How to respond to an Attack-Tips to Avoid Being a VictimBUY THIS BOOK NOW AND GET STARTED TODAY!

Social Engineering Penetration Testing Gower Publishing, Ltd.
What are social policies? How are social policies created and implemented? Why do certain policies exist? The fourth edition of this highly respected textbook provides a clear andengaging introduction to social policy. The book has been thoroughly updated to include: Changes in social policy introduced by the Coalition government Incorporation of an international perspective throughout, as well as anew chapter: The global social policy environment Updated pedagogy to stimulate thought and learning Comprehensive glossary Social Policy is essential reading for students beginning or building on theirstudy of social policy or welfare. The wide-ranging coverage of topics meansthat the book holds broad appeal for a number of subject areas includinghealth, social policy, criminology, education, social work and sociology. "This textbook has always been a useful teaching resource because it combines substantial and engaging analysis with 'stand alone' extracts. The new edition adds a chapter on global social policy, updates on the Coalition Government and guides to what is in the book. The added activities are well thought out and can be adapted or expanded to suit the needs of particular students." Hedley Bashforth, Teaching Fellow in Social Policy, University of Bath,

UK "Social Policy: An Introduction, now in its fourth edition and eleventh year, will remain a core social policy text on reading lists across the country due to its well written and comprehensive nature. Completely revised, it has been updated and extended to reflect contemporary developments in social policy, including the policy implications of the Coalition Government, and now includes a chapter on global social policy environments reflecting the continued internationalisation of social policy debates. Updated pedagogical features, which include activities for the reader, learning outcomes at the start of each chapter and detailed case studies throughout, enhance this thought-provoking and stimulating text." Dr Liam Foster, University of Sheffield, UK "This book provides, as it states, an introduction to the field and does so by adopting a highly attractive pedagogic style that evidences, at every turn, a sensitivity to the approaches to learning of contemporary students. Although it is tailored to meet the needs of primarily first year specialist students, it is equally suitable for those on other programmes who are taking an option in social policy. Because the book anticipates theoretical issues and debates and students will confront as they progress to a more advanced level, it will also retain value as be a longer-term reference resource. I will certainly be citing it on a second year core course I teach. It is immediately clear that a great deal of thought has been invested into designing this book. What Blakemore and Warwick-Booth have produced is a clearly laid out and well-structured analysis of impressive breadth that is a readily accessible learning instrument both for student and teacher. Importantly, it provides numerous opportunities to experiment with new ways of approaching the teaching of the subject. Each chapter sets out clearly expressed learning outcomes with a fair balance of theoretical and empirical concerns. Visual displays in box material, graphs and flow charts provides a most effective means for absorbing the large amount of ground covered. There is good incorporation of statistical material and up to date policy developments. Students are also encouraged to exploit useful links to internet and other media sites. Particularly attractive from a teaching point of view are the range of tasks set for the students which are aimed clearly at rapid capacity building. Chapters end by listing the key terms and concepts addressed to aid revision of material. This is repeated in the glossary at the end of the book. Most of the materials are derived from the British context, but there is also a secondary focus on EU member states and beyond, as well as a good chapter on global social policy." Steen Mangen, Department of Social Policy, London School of Economics and Political Science, UK

Social Engineering Lulu.com

The Social Engineer's Playbook is a practical guide to pretexting and a collection of social engineering pretexts for Hackers, Social Engineers and Security Analysts. Build effective social engineering plans using the techniques, tools and expert guidance in this book. Learn valuable elicitation techniques, such as: Bracketing, Artificial Ignorance, Flattery, Sounding Board and others. This book covers an introduction to tools, such as: Maltego, Social Engineer Toolkit, Dradis, Metasploit and Kali Linux among others. Crucial to any social engineering test is the information used to build it. Discover the most valuable sources of intel and how to put them to use.

Seven Deadliest USB Attacks Elsevier

This encyclopedia spans the relationships among business, ethics and society, with an emphasis on business ethics and the role of business in society.

CompTIA Security+ SY0-301 Practice Questions Exam Cram "O'Reilly Media, Inc."

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.

Social Engineering Springer

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.