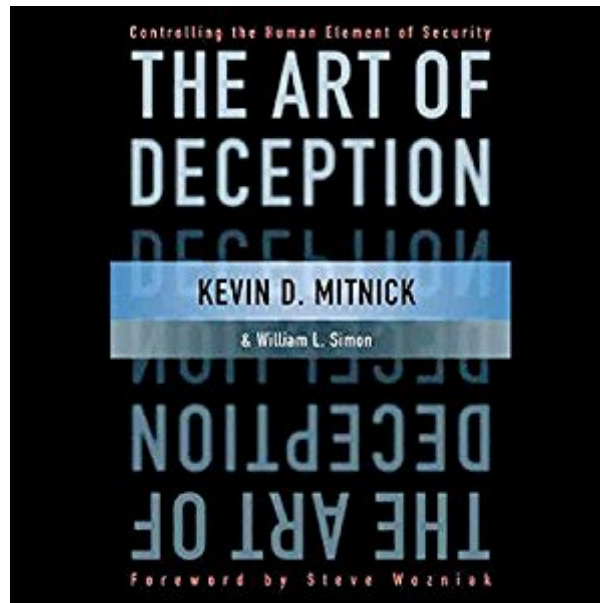The book was found

The Art Of Deception: Controlling The Human Element Of Security

Synopsis

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. --This text refers to the Paperback edition.

Book Information

Audible Audio Edition

Listening Length: 13 hours and 41 minutes

Program Type: Audiobook

Version: Unabridged

Publisher: Audible Studios

Audible.com Release Date: July 28, 2009

Whispersync for Voice: Ready

Language: English

ASIN: B002JF132I

Best Sellers Rank: #46 in Books > Audible Audiobooks > Nonfiction > Computers   #79 in Books > Business & Money > Management & Leadership > Information Management   #89 in Books > Computers & Technology > Security & Encryption

Customer Reviews

"The Art of Deception" was recommended to me by an instructor teaching a CISSP prep class. It is both an enjoyable and informative read. Mitnik is the "real deal" in exploiting social engineering techniques and his books should be required reading by corporate security policy makers (and I am sure it is for many already).This book illustrates various techniques for bypassing established corporate physical and information security security policies. I have actually inadvertently used some of these techniques when troubleshooting network issues or having forgotten my passcard to gain access to systems and rooms. It is often easier to bypass the rules than to go through the steps needed to obtain proper access and people are surprisingly willing to cooperate "just this one time".This book will help you sensitize your employees to the risks of bypassing security policy and recognize when this might be occurring.Highly recommended!CFH

OK read.

After reading it, the book makes one more aware of what to be careful when giving out information of any kind and how to protect yourself and your company's assets. I've heard alot of "Don't ever give out your id/password", "Always have firewalls on your network." One hardly ever hears about 'make sure you're giving information to someone who's supposed to have it'. There's tons of books on security with respect to technology but this is the first one I've seen that actually focuses on the weakest link when it comes to security - the human element.All the firewalls and software can't prevent a social engineer from getting in if he/she knows justs how to act and/or what to say to get what they want. Reading the scenarios really opened my eyes. Theres a scenario where a social engineer pretended to be a manager of a video store. After enough talking to another employee at another branch, the social engineer was able to get enough information to obtain the credit card # of someone who owed money to the client the social engineer was hired by.In reading the scenarios, I'd seen examples where I'd asked for the type of information described for perfectly legitimate reasons. I'd never imagined how someone could take just 1 or 2 pieces of information and create chaos for a person or a company. If you're in the IT industry, or work in any kind of customer service, you really need to pick up this book. This book doesn't bash people for being as helpful as they can be (team player, etc). He's just saying to be more aware of what's going on and when giving out any kind of information, being a little cautious doesn't hurt. As humans, we're not perfect to begin with, but a little awareness will make it just a little harder for that social engineer to get what they want.

Ghost in the Wires is way better and ruins this book if read after.

Very comprehensive and informational, Kevin knows his security and its scary in one respect that systems all have some way of being broken afterall they were designed by humans. I like how its written its captivating and uses lots of story lines to back up the topics of the book.

great book

Kevin Mitnick has been arguably the most famous computer hacker out there. His story has been told by others in several books. But here Mitnick is not trying to really share his experiences - rather he calls upon his collection of acquaintances and others he knows to illustrate how people can be engineered. Most of the book is essentially a series of stories of social engineering (getting someone to do what you want without their realizing it) and then some superficial analysis of why it worked. He then tries to synthesize his earlier chapters into a set of practical security precautions, many of which are common sense, and most of which the reader would have already figured out from reading the book. The stories he chooses to share are fairly interesting, both in their daring and setup and in their simplicity. What this book would be best for would be handing it to a corporate manager and allow him or her a wake up call as to security. As we try to work together, have things automated and available on-line and as our organizations grow the catchword is results, even if you have to bend the rules a bit. This is what the social engineer can exploit. Many of the stories skate along the edge of the law, and Mitnick points out when it would cross into illegal. While interesting, after a while the book becomes more tedious in structure and what is being said. Still it is very accessible and would be a great book for someone not so familiar with computers and hacking to see how some of it is done. It should serve as a wake-up call for management as to some of the dangers we face every day. And while most of the stories presented are more in the spirit of curiosity, or fun, or revenge, it would be easy to take them up a notch into activities with serious corporate impact.

This is the first book that I've read from cover to cover in close to 7 years. I could not put it down! Read it in 2 weeks, taking notes, evaluating the way I responded to calls at my companies help desk, reviewing some of the links mentioned in the book, etc., etc.,etc. This is one book that if you read it you will have the ability to better defend and better compromise anything and anyone, but if you don't read it you will eventually regret it because there is a wealth of information that I haven't

found anywhere else. There are popular web links mentioned that I was shocked to find were still valid. The detail and instruction are immaculate and if you don't read it....simply put you are a foolish morron. Headlines should read, "Mitnick does it again with a simple Mitnick Message!". Kevin, you inspire me and I wish I had your knowledge and influence.

Download to continue reading...

The Art of Deception: Controlling the Human Element of Security Social Security & Medicare Facts 2016: Social Security Coverage, Maximization Strategies for Social Security Benefits, Medicare/Medicaid, Social Security Taxes, Retirement & Disability, Ser Mind Control Mastery 4th Edition: Successful Guide to Human Psychology and Manipulation, Persuasion and Deception! (Mind Control, Manipulation, Deception, ... Psychology, Intuition, Manifestation,) The Handbook of Five Element Practice (Five Element Acupuncture) The Finite Element Method: Linear Static and Dynamic Finite Element Analysis (Dover Civil and Mechanical Engineering) Human Systems Integration to Enhance Maritime Domain Awareness for Port/Harbour Security: Volume 28 NATO Science for Peace and Security Series - D: ... D: Information and Communication Security) Security Camera For Home: Learn Everything About Wireless Security Camera System, Security Camera Installation and More Nuclear Safeguards, Security and Nonproliferation: Achieving Security with Technology and Policy (Butterworth-Heinemann Homeland Security) Fundamentals Of Information Systems Security (Information Systems Security & Assurance) - Standalone book (Jones & Bartlett Learning Information Systems Security & Assurance) Nursing: Human Science And Human Care (Watson, Nursing: Human Science and Human Care) The Missing Element: Inspiring Compassion for the Human Condition The Command to Look: A Master Photographer’s Method for Controlling the Human Gaze Controlling Human Heredity: 1865 to the Present (Control of Nature) Mind Control, Human Psychology, Manipulation, Persuasion and Deception Techniques Revealed. (dark psychology, mind control, hypnosis, forbidden psychology, manipulation)) Mind Control, Human Psychology, Manipulation, Persuasion and Deception Techniques Revealed MIND CONTROL: Manipulation, Deception and Persuasion Exposed: Human Psychology (Manipulation, Hypnosis, Brainwashing, Subconscious Mind, Psychopath) Mind Control Mastery 4th Edition: Successful Guide to Human Psychology and Manipulation, Persuasion, and Deception! Off Speed: Baseball, Pitching, and the Art of Deception Polymer Clay Gemstones: The Art of Deception The Art of Deception: An Introduction to Critical Thinking

Privacy

FAQ & Help