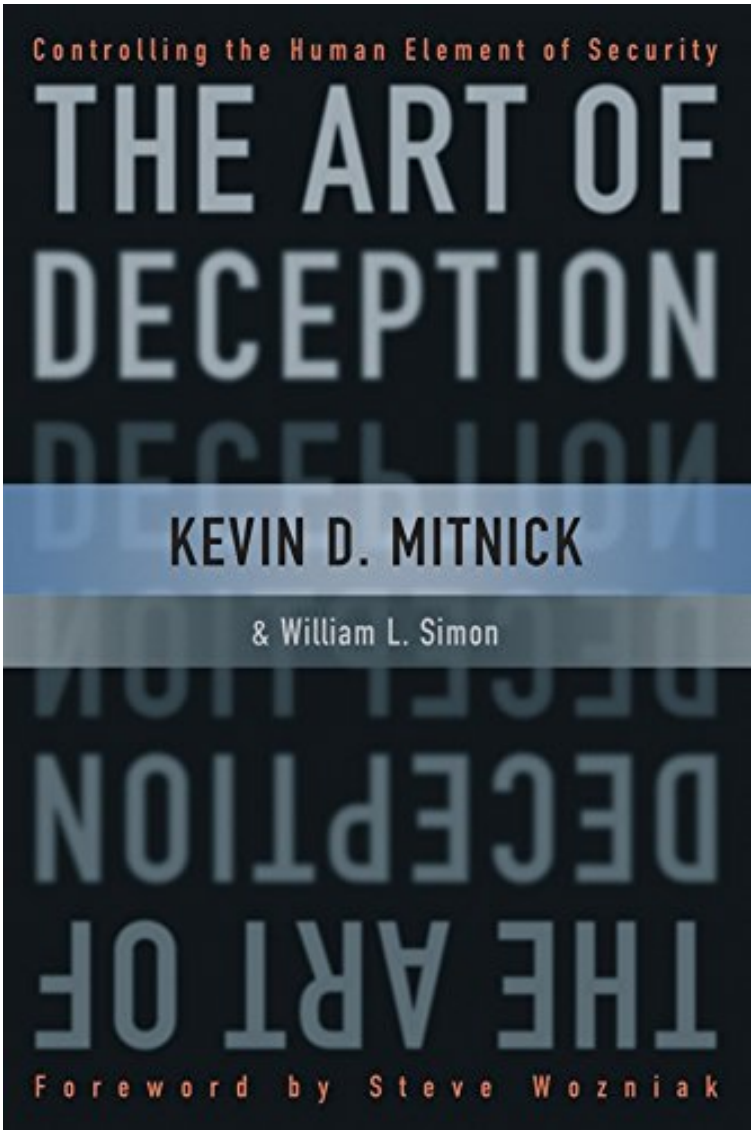
The Art of Deception: Controlling the Human Element of Security

Kevin D. Mitnick, William L. Simon
*ebooks | Download PDF | *ePub | DOC | audiobook*



#53761 in eBooks 2007-08-20 2007-08-20File Name: B006BBZHAK | File size: 72.Mb

Kevin D. Mitnick, William L. Simon : The Art of Deception: Controlling the Human Element of Security before purchasing it in order to gage whether or not it would be worth my time, and all praised The Art of Deception: Controlling the Human Element of Security:

0 of 0 people found the following review helpful. Social Engineering 101 - Highly RecommendedBy C. Hill"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!CFH2 of 2 people found the following review helpful. Speaks volumes on social engineering/makes you think!By EAfter 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.0 of 0 people found the following review helpful. Two StarsBy Reza QinGhost in the Wires is way better and ruins this book if read after.

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.