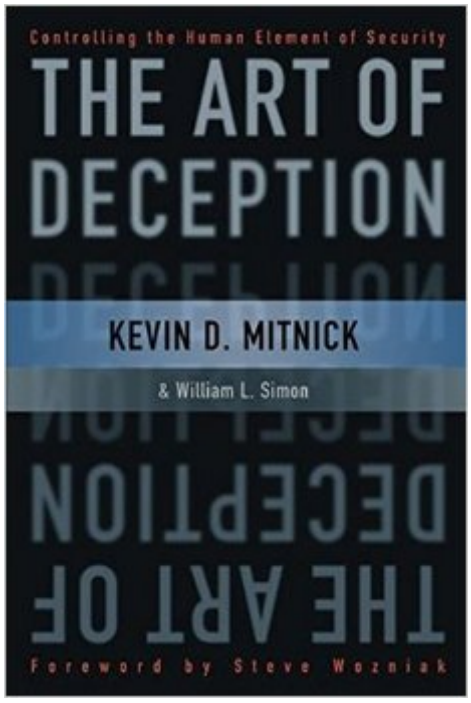
The Art Of Deception: Controlling The Human Element Of Security



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.

Book Information

Paperback: 368 pages

Publisher: Wiley; 1 edition (October 17, 2003)

Language: English

ISBN-10: 076454280X

ISBN-13: 978-0764542800

Product Dimensions: 6 x 1 x 9.1 inches

Shipping Weight: 1 pounds (View shipping rates and policies)

Average Customer Review: 4.2 out of 5 starsÂ Â See all reviewsÂ (204 customer reviews)

Best Sellers Rank: #30,977 in Books (See Top 100 in Books) #14 inÂ Books > Computers & Technology > Certification > CompTIA #31 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Security #37 inÂ Books > Computers & Technology > Internet & Social Media > Hacking

Customer Reviews

Mitnick has his own reputation to live up to with this book, which sets a pretty high bar for the

audience who knows him as the "World’s Most Notorious Hacker." Unfortunately, while he knows the material cold, his skills as an author are less stellar.The vignettes describing various cons are, in the large, very entertaining. They’re fictionalized, and sometimes the dialogue feels artificial. This book is supposed to convince us how easily people are victimized by social engineers. When the victim’s dialogue plays too obviously into the con man’s hands (for the purpose of illustrating the point relevant to the enclosing chapter/section), this goal is to some extent defeated. It’s too easy to read unnatural dialogue and use that as an excuse to tell oneself, "I don’t have to worry about that sort of attack -- I’m not that dumb!" More effort could have been expended in fictionalizing these scenarios without making them so difficult to relate to. Seeing how a con is performed is kind of like learning how a magic trick works -- it holds a similar fascination. Imagine seeing an amazing magic trick performed on television, wondering how it was possibly accomplished, and then learning that the trick was all in the video editing. That really sucks the fun out of the magic -- analogously, when the "trick" in one of these cons is just that the victim does something obviously stupid at just the right moment, the believability and enjoyment are damaged.Despite what I’ve said, the cons are definitely enjoyable to read and do offer some genuine insights. Not all suffer from believability problems. However, the supporting material discussing these scenarios is pretty weak. There’s a rigid format ("Analyzing the con," "Preventing the con," etc.

Kevin Mitnick says "the term ’social engineering’ is widely used within the computer security community to describe the techniques hackers use to deceive a trusted computer user within a company into revealing sensitive information, or trick an unsuspecting mark into performing actions that create a security hole for them to slip through." It’s suitable that Mitnick, once vilified for his cracking exploits, has written a book about the human element of social engineering - that most subtle of information security threats.Some readers may find a book on computer security penned by a convicted computer criminal blasphemous. Rather than focusing on the writer’s past, it is clear that Mitnick wishes the book to be viewed as an attempt at redemption.The Art of Deception: Controlling the Human Element of Security states that even if an organization has the best information systems security policies and procedures; most tightly controlled firewall, encrypted traffic, DMZ’s, hardened operating systems patched servers and more; all of these security controls can be obviated via social engineering.Social engineering is a method of gaining someone’s trust by lying to them and then abusing that trust for malicious purposes - primarily gaining access to systems. Every user in an organization, be it a receptionist or a systems administrator, needs to know that when someone requesting information has some knowledge about company procedures

or uses the corporate vernacular, that alone should not be authorization to provide controlled information.The Art of Deception: Controlling the Human Element of Security spends most of its time discussing many different social engineering scenarios.

I waited for the book of the famous hacker Kevin Mitnick for a longtime, checking my mailbox every day after my pre-order wascompleted. The book was almost worth the wait!Its a fun book with lots of entertaining and education stories on whatis possible by means of social engineering attacks. The characterclearly push the limits of this "human technology".One of the articles I have read on the book called it "Kevin Mitnick'sLatest Deception" due to his downplaying of technology securitycontrols and emphasizing people skills and weaknesses. However, thehuman weaknesses do nullify the strengths of technology defenses andhumans are much harder to "harden" than UNIX machines.The attack side is stronger in the book than the defense side,naturally following from the author's background. However, there aresome great defense resource on policy design, awareness and neededvigilance. However, there is this "minor" issues with defense againstsocial engineering: one of the definitions called it a "hacker'sclever manipulation of the natural human tendency to trust". The word"natural" is key; if we are to believe the definition, all defensesagainst social engineering will be going against _nature_ and, as aresult, will be ineffective for most environments. Author alsoadvocates social engineering penetration testing, which appears to bethe best way to prepare for such attacks. Security awareness, whileneeded, will get you so far.

Edition) Codependent No More: How to Stop Controlling Others and Start Caring for Yourself Proactive Risk Management: Controlling Uncertainty in Product Development Active Portfolio Management: A Quantitative Approach for Producing Superior Returns and Controlling Risk Project Management: A Systems Approach to Planning, Scheduling, and Controlling Codependent No More, by Melody Beattie: Key Takeaways, Analysis, & Review: How to Stop Controlling Others and Start Caring for Yourself Why Does He Do That?: Inside the Minds of Angry and Controlling Men Atkins Diabetes Revolution CD: The Groundbreaking Approach to Preventing and Controlling Diabetes The Food Service Professional Guide to Controlling Restaurant & Food Service Operating Costs (The Food Service Professional Guide to, 5) (The Food Service Professionals Guide To) The Food Service Professional Guide to Controlling Restaurant & Food Service Food Costs (The Food Service Professional Guide to, 6) (The Food Service Professionals Guide To)