

**The Art of Deception:
Controlling the Human Element of Security
Written By Kevin D. Mitnick and William L. Simon
Reviewed By John B. Moretta**

At a time when we face incessant threats to our national, personal, and corporate security Kevin Mitnick's innovative and insightful new book, *The Art of Deception: Controlling the Human Element of Security*, provides a clear view into the inevitable problems we face in preventing such invasions and also outlines several practical approaches that can help to prevent such attacks. The 339-page hard cover book addresses security problems in a practical manner complete with real life stories from Mitnick's personal experiences. The book should be required reading for every individual and corporation concerned about the privacy and confidentiality of its computer and phone systems.

Mitnick, a well known "cyber desperado" and former fugitive was released from federal prison in 2000. Prior to his imprisonment Mitnick preyed on strangers in an effort to gain access to highly confidential information by finding vulnerability in operating systems. Achieving success in these endeavors at a very young age, Mitnick's exploits continued to grow to unprecedented heights until his arrest and imprisonment. Since his release, Mitnick has acknowledged the illegal nature of his actions and focused on providing solutions and guidance to help others avoid attacks similar to those he previously committed.

Mitnick begins *The Art of Deception* by providing the reader with an insightful view into his own background and experiences as a "hacker" and "con man." In doing so, Mitnick, a self characterized "social engineer," offers his personal

definitions of these terms and gives the reader a grasp on what characterizes this curious, intelligent, and surreptitious sub culture of individuals. The personal stories that Mitnick shares in the book enable the reader to step into the mind of the “con man,” if only for a second, to explore the intricate details and planning that comprise a successful attack. After doing so, it becomes clear that these “hackers,” “con men,” and “social engineers,” are not all that different from you and me. Instead, Mitnick shows the reader that many of the characteristics that drive individuals to become successful entrepreneurs, businessmen and women, and professionals in their field, are the same traits that drive these “hackers”: curiosity, persuasion, influence, and a desire for a good intellectual challenge.

After providing the reader with an in depth view of those who toil in our operating systems, Mitnick segues into a lengthy and detailed analysis of society’s most vulnerable points and explains how to avoid such precarious situations. He focuses on human nature as the pivotal reason for most security breakdowns and explains that our need for absolute security oftentimes leads us to settle for a false sense of security. As a result of this false perception, corporations and individuals are at an increased risk of attack because they fail to explore many scenarios that could lead to security breaches. The corporate illusions fostered by this feeling of absolute security are often based on expensive and robust security mechanisms that are highly susceptible to attack.

Throughout the remainder of the book Mitnick mixes a continuing exploration of the social engineer’s mindset with blurbs aptly entitled “Mitnick Messages” and “Lingo.” The brief, highlighted paragraphs appear in key sections of the book and assist the reader in

deciphering the jargon surrounding the subject matter of the various chapters and offer valuable tips to the reader as a summation of the section they have just read.

Mitnick's approach throughout this book is extremely practical, well written, and easy to understand. It places the reader in a position that allows them to gain an understanding of the social engineer's goals and intentions, and helps the reader to develop proactive strategies to deal with these individuals. Accordingly, this book is a must read for not only those individuals responsible for maintaining corporate security but also for those who wish to gain a better understanding of human nature and our innumerable inadequacies in protecting ourselves and our privacy.