

Mitnick Security Consulting, LLC
2245 N Green Valley Pkwy #411
Henderson, NV 89014
702.940.9881

Kevin Mitnick



Testimonials:

"Mr. Mitnick's presentation was not only informative and entertaining; it also brought home some very relevant information security issues. The audience was captivated by his live demonstration of what information is available at the click of a mouse."

Teresa Rojas -- Acting Director
Office of Systems Security
Operations Management
Social Security Administration

"Kevin Mitnick delivered an engaging message of real life stories and live demos to an audience of over 500 at our annual Technology Celebration Banquet hosted by the Applied Information Management Institute. It's both frightening and informative to hear how effective social engineering can be in assessing what should be security sensitive information. If anyone left not a little more cautious or a little more paranoid, they missed an excellent delivery."

Scott Pettit
VP of Business Services
The AIM Institute

"Mitnick left his audience shaken, but better equipped to stave off attacks via social engineering."

Norm Staniford
Account Executive
Computer Sciences Corporation

"Thanks, Kevin for allowing us to use the video clip of your interview discussing some of the security issues that every organization should be aware of. Your video clip will be a part of the Fiscal Year... Information Systems Security (SSI) Awareness Training Course that we're mandated by public law to provide all Federal Aviation Administration (FAA) employees and contractors."

Michael F. Brown, AIS-1
Director
Office of Information Systems Security
US Department of Transportation/FAA

BIOGRAPHY:

With more than fifteen years of experience in exploring computer security, Kevin Mitnick is a largely self-taught expert in exposing the vulnerabilities of complex operating systems and telecommunications devices. His hobby as an adolescent consisted of studying methods, tactics, and strategies used to circumvent computer security, and to learn more about how computer systems and telecommunication systems work.

In building this body of knowledge, Kevin gained unauthorized access to computer systems at some of the largest corporations on the planet and penetrated some of the most resilient computer systems ever developed. He has used both technical and non-technical means to obtain the source code to various operating systems and telecommunications devices to study their vulnerabilities and their inner workings.

As the world's most famous (former) hacker, Kevin has been the subject of countless news and magazine articles published throughout the world. He has made guest appearances on numerous television and radio programs, offering expert commentary on issues related to information security. In addition to appearing on local network news programs, he has made appearances on 60 Minutes, The Learning Channel, Tech TV's Screen Savers, Court TV, Good Morning America, CNN's Burden of Proof, Street Sweep, and Talkback Live, National Public Radio, and as a guest star on ABC's spy drama "Alias". Mitnick has served as a keynote speaker at numerous industry events, hosted a weekly talk radio show on KFI AM 640 in Los Angeles, testified before the United States Senate, written for Harvard Business Review and spoken for Harvard Law School. His first best-selling book, The Art of Deception, was published in October 2002 by Wiley and Sons Publishers. His second title, The Art of Intrusion, was released in February 2005.

THE ART OF DECEPTION: ARE YOU IN DANGER OF BEING 'CONNED'?

Join us to hear the world's most famous former hacker share his perspective on the threat of "social engineering"-a highly effective type of attack that exploits the human element of corporate security.

While relatively unknown to the general public, 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.

Mitnick illustrates why a misplaced reliance on security technologies alone, such as firewalls, authentication devices, encryption, and intrusion detection systems are virtually ineffective against a motivated attacker using these techniques.

Although there are no reported statistics on the number of successful social engineering attacks, these age-old techniques have been and continue to be extremely effective against unsuspecting targets, and pose the least risk and cost to your adversary.

In the corporate environment, a large number of unsuspecting victims never realize they have been manipulated. Will your employees be the next? Through concrete examples, Mitnick shares what your business can do to develop a creative and engaging security program that heightens awareness, motivates employees to change their attitudes, influences them to think defensively, and encourages the adoption of good security habits.

THE ART OF INTRUSION: HOW HACKERS COMPROMISE YOUR SECURITY AND WHAT YOU CAN DO ABOUT IT...

To truly protect your organization's valuable information, you must move beyond knowledge of the dangers and learn from real, "you are there" case studies shared by Mr. Mitnick himself. Kevin Mitnick, the world's most famous (former) hacker, spent several years gleaning insights from the hacker community and gathering critical lessons-learned.

In this dynamic and riveting presentation, Mr. Mitnick shares how hackers ply their trade and offers concrete and actionable guidance to help you strengthen your defenses.

He'll reveal the hair-raising details of real-life computer break-ins, how the perpetrators hacked in and how they successfully covered their tracks. More importantly, Mr. Mitnick will share how you can prevent these same horror stories from being repeated in your organization. In addition, you will learn cost-effective counter measures and indispensable tips for bringing everyone in your organization on-board to offer maximum protection.

WIRELESS INSECURITY: IS YOUR NETWORK VULNERABLE?

The use of wireless networking is becoming ubiquitous throughout the world. Countless businesses, government agencies, academic institutions, and telecommuters have deployed wireless networks in their computing environment. As a result, those organizations have opened up their networks to data thieves, vandals and hackers.

The real danger starts with the IT implementers who may not accurately assess the risks involved in the deployment of wireless technologies. Lulled into a false sense of security, many organizations believe the risks associated with their wireless connectivity is minimal based on the belief that these wireless signals only extend to the four walls of their organization or facility.

Join us to hear Kevin Mitnick discuss why this thinking is creating rampant insecurity in wireless networks, and learn just how easy it is for anyone with a computer and wireless card to breach these networks. During his presentation, Mr. Mitnick will demonstrate the tools and techniques that hackers are using everyday to compromise the security of numerous enterprises and consumers.

Mr. Mitnick will also share specific guidance you can immediately put to use to raise the bar of organizational awareness and mitigate the risk that your wireless network will be the next stepping stone into sensitive corporate data and computing resources.

THE TRUTH BEHIND THE MYTH OF KEVIN MITNICK

Most people's concept of the 'real' Kevin Mitnick is derived from media-created myths. The media created a fantastic story and credited him with activities being carried out by other hackers, because if there was one villain, the story was much more interesting. The more interesting the story, the more newspapers and magazines it could sell.

Kevin Mitnick has been fascinated with technology since early childhood. His dabbling in electronics began with CB and ham radios. He eventually graduated to manipulating the phone system to play pranks on people, after the hobby of phone phreaking was introduced to him by some high school friends. Mitnick was intrigued by the phone systems, and had a desire to know everything about how they worked. When the phone systems converted over to computerized, switches, he graduated along with them, and approached computers with the same vigor with which he had mastered the phone system.

Kevin was never a malicious hacker and his hacking was never performed for personal gain or to cause damage to systems. His pursuit of hacking was purely to satisfy his intellectual curiosity, and, contrary to many inaccurate reports, he never destroyed data or profited from his exploits.

Unfortunately, the government could not understand a hacker who was motivated by a personal quest for knowledge and a good challenge. Since computer crime was a relatively new challenge for the government back in the mid-1990's, there were major efforts to obtain funding for these new crime-fighting programs. These programs couldn't get the funding without the public's support. This drive for funding, combined with the sensationalist media reports depicting Kevin as the Most Wanted Hacker in the World, was all the government needed to make Kevin Mitnick their prime target.

Kevin describes how he won the "scapegoat sweepstakes" based on the intense fear and propaganda generated by the American media and the U.S. government. You will hear first hand about what he did and why he did it, and his experiences at the hands of the United States criminal justice system.