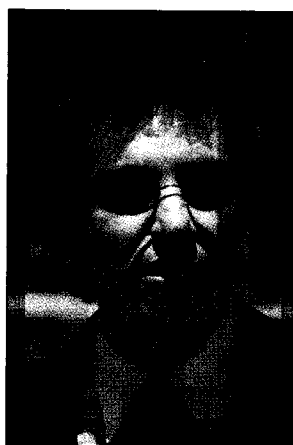


Unlikely Security Advice BY AL BERG

Just days after federal officials removed a gag order preventing notorious ex-cracker Kevin Mitnick from advising anyone on computer- or Internet-related matters, Mitnick began plying his new trade: security consultation. Though the terms of his probation still prevent him from leaving Southern California, Mitnick participated by telephone in an infosecurity session at last month's H2K, a hacker convention in New York City. Mitnick didn't talk technology, but instead outlined techniques (and preventive measures against) what is arguably the most powerful



Kevin Mitnick

tool in the computer criminal's arsenal: social engineering. Social engineering, for the uninitiated, is the extraction of confidential information from employees of a targeted organization simply by talking to them. The old "I'm calling from the IT department and I need your user name and password" ploy is social engineering in its most basic form. (Mitnick says he used that approach on "only one or two occasions...because that's such a red flag.")

Many of Mitnick's exploits involved large organizations, including phone companies. He spoke of being able to take advantage of "the size of the organization and the number of people who

worked there. If you learned the lingo and did some homework and intelligence gathering, it was quite simple to manipulate them," he said.

While the level of the technical threat that Mitnick presented to the Free World is still in dispute, his skills as a con man seem to have been a key to many of his attacks. "You try to make an emotional connection with the person on the other side.... Usually I did it all by improv.... I would establish some sort of degree of trust with the person I was speaking with." The attacker just needs to know *something* about the organization, and the bravado to play upon it. "Get some names, get some extensions, try and find out who is on vacation, who manages what projects," Mitnick advised would-be attackers.

Okay, but what about the other side of the fence—the security guy who's trying to protect against social engineering attacks? Towards the end of the session, I asked Mitnick for a few tips. He offered a number of suggestions:

- Teach employees to "question anyone they don't know when they get a phone call."

- "Put a verification mechanism in place for employees to use if they don't recognize a person [calling for information]."

- Put a message on your main phone number stating that calls may be monitored and taped for quality assurance. "This is a real deterrent, since you don't know if you are being taped or not."

The bottom line? According to Mitnick, "It all comes down to user awareness and education.... Show employees how they could potentially be a 'mark.'" ♦

AL BERG (al@al-berg.com) is a security consultant with Mentor Technologies.

Mitnick Again?

It was with great disdain and trepidation when I read the news section in the August issue, ("*Unlikely Security Advice*," www.infosecuritymag.com/aug2000/news.htm), only to find another rendition of the "Incredibly Talented Mr. Mitnick." I can only assume Al Berg was using some editorial tongue-in-cheek in giving a criminal such as Mitnick any legitimacy in the information security business.

I was even more disturbed earlier this year when Mr. Mitnick appeared before Sen. Fred Thompson's and Rep. Steve Horn's congressional oversight committees and was recognized as an information security practitioner. Other than his well-chronicled exploits as a cyber-counter culture icon, what credentials does he hold? I would certainly like to see Mitnick match wits with the CISSP test—although I am sure he could social engineer his way through and really be accepted into the information security fraternity. It's a sad day when corporate and government leadership anoint a criminal with such high status in the face of the thousands of legitimate information security professionals. But then again, they are the same leaders who ignore us until the infamous middle-of-the-night phone call awakens them to yet another DDoS, ILoveYou virus or malicious intrusion.

Bottom line—I really expected more from a trade publication that represents the true professionals.

Robert S. Jack II

AL BERG RESPONDS:

Thanks for your feedback about my article on Kevin Mitnick's "tele-appearance" at H2K.

When I wrote the piece, I took pains not to paint a picture of Mitnick as a talented techie, but as a talented con man. I just re-read the piece and still think that this attitude comes through in it. I chose to write the article about Mitnick for two reasons: first, because his exploits are based on social engineering rather than technical skill; and second, because Mitnick's notoriety would encourage readers to read the article and become more aware of the dangers of social engineering.

I don't like computer criminals any more than anyone else, but I feel that they are part of the information security landscape and do offer us some lessons. Hence my attendance at and reporting on events such as H2K and DefCon.