

TECHNOLOGY

ONLINE SECURITY SPECIAL REPORT

[» Overview](#) | [Quiz](#) | [Secure your network](#)

A convicted hacker debunks some myths

Thursday, October 13, 2005 Posted: 1911 GMT (0311 HKT)

(CNN) -- To many, the name Kevin Mitnick is synonymous with hacking, the cinematic sort where a snot-nosed kid thumbs his nose at authority. But, Mitnick says, the characterization is a bit overdone and the legend untrue, if not libelous.

It is true, he says, that he broke into corporate computer systems and stole source code to satisfy his curiosity, but he denies the stories that he hacked into NORAD -- North American Aerospace Defense Command -- or that he wiretapped the FBI.

After a well-publicized pursuit that made him notorious, the FBI arrested Mitnick in 1995. He served five years in prison after pleading guilty to charges of wire and computer fraud. He was released in 2000 and today runs a computer security firm. In a telephone interview with CNN's Manav Tanneeru, Mitnick talks about his past, the state of online security today, and how he handles what his name has come to mean.

CNN: There is a certain myth of Kevin Mitnick, but you seem to disavow a lot of it. Why exactly did you become so famous and what specifically was reported that was inaccurate?

MITNICK: [The claims] that I wiretapped the FBI or something like that were something out of a movie like "War Games" or "Enemy of the State" or something. There were fictional events that were tied to real events, like when I took code from Motorola and Nokia when I was a hacker to look at the source code. I took a copy, which is essentially stealing, to look at the information. That was true, that was the truth ... in the story, but there were a lot of libelous statements. ...

I'm the one that got myself into trouble, but because the reporting in the [New York] Times portrayed me as this very dangerous character, the government stepped up the prosecution of the case.

At the end of the day, I would have been prosecuted, but I wouldn't have been held in solitary confinement for a year for the fear that I could launch nuclear missiles by whistling through a pay phone.

I was powerless because I was represented by a publicly appointed attorney who had a very limited budget. But a lot of accusations I wasn't charged with. If I hacked into NORAD or wiretapped the FBI, I certainly would have been charged with it. I got into trouble largely because of my actions. However, because of the media reporting, I was treated as "Osama bin Mitnick."

CNN: You were once the most famous and sought after hacker in the country. After your release from prison you were asked to testify before the Senate, and you now run a Web security firm, which is a fascinating evolution.

MITNICK: It's kind of interesting, because hacking is a skill that could be used for criminal purposes or legitimate purposes, and so even though in the past I was hacking for the curiosity, and the thrill, to get a bite of the forbidden fruit of knowledge, I'm now working in the security field as a public speaker. Twenty-five percent of my revenue is actually doing security assessments, so people actually hire [me] to break into their systems to find their security failures and patch them before the bad guys find them.

So, it's kind of interesting, because what other criminal activity can you ethically practice? You



Kevin Mitnick

SPECIAL REPORT



- [Overview](#)
- [Quiz](#)
- [Secure your network](#)
- [Special Report](#)

YOUR E-MAIL ALERTS

Kevin Mitnick

Computer Security

Technology (general)

Hackers

or [Create Your Own](#)

[Manage Alerts](#) | [What Is This?](#)

can't be an ethical robber. You can't be an ethical murderer. So it's kind of ironic. But it is really rewarding to know that I can take my background and skills and knowledge and really help the community.

CNN: The fact that you are back in the online world, especially the cyber security sector, may give many reason for a certain insecurity and paranoia. How has your firm been received?

MITNICK: There are several in the security field that don't trust me. They're my competitors, and right there, there is an agenda. But I'm sure that our company does not receive phone calls because they're concerned about my past, and then again, there are a lot of people that do make those calls, and they keep the business going pretty good. I never got a phone call saying, "Hey, we're not hiring your firm because of x, y and z."

I don't know what the percentage is, but I'm sure there are people that don't want to use our firm because they really don't know much about the case. They just know me as a hacker that went to jail.

CNN: Compared to the time you were an illegal hacker, and the contemporary landscape, how easy is it to hack a computer? Has security improved much? Would you still be able to do what you did years ago?

MITNICK: I get hired to hack into computers now and sometimes it's actually easier than it was years ago. It really depends on who the client is -- or if you're doing ethical hacking, who the target is. It could be a difficult target or an easy target. The security landscape, the only thing that's changed in regards to vulnerability are technical issues, but with social engineering, it's all remained the same. So, it depends how vigilant the owners and the operators of the computer systems and the network are, and it really doesn't go to the question of are we living in a more secure world?

CNN: Then, how vulnerable is the common user? Sure, it depends on how many safeguards they've installed, but if they have the most effective of security, how easy is it?

MITNICK: I did a study USA Today was involved with and another marketing firm in San Francisco was involved with within the last year, and we set up a honeypot network, which was six different networks running various different operating systems. We plugged them into a DSL line in San Francisco, and we just watched them to see how quickly these systems could get broken into without having any protection. And one of the computers was broken into four minutes after plugging it into the Internet, which is quite astounding.

CNN: You previously mentioned social engineering. What exactly does that term mean to you?

MITNICK: Social engineering is using manipulation, influence and deception to get a person, a trusted insider within an organization, to comply with a request, and the request is usually to release information or to perform some sort of action item that benefits that attacker. It could be something as simple as talking over the telephone to something as complex as getting a target to visit a Web site, which exploits a technical flaw and allows the hacker to take over the computer.

CNN: And how do contemporary hackers use social engineering in what they do?

MITNICK: Well, how about Paris Hilton? She was attacked on her cell phone, and she was attacked two ways. One was because of a T-Mobile's Web site, and the other guy was able to compromise it by getting her phone number by going on T-Mobile's Web site, doing a password reset, which SMS-ed her new password because, presumably, only the owner would have the handset.

And then what they did was, they did a technique called caller ID spoofing, which allows a person to change the number they're calling from on their calling phone number display. So, they were posing as T-Mobile customer service, and they called her phone, and on the caller ID it showed as T-Mobile customer service, and then they told her, "There are some network difficulties. Have you been getting any SMS [messages] about a password reset, and what were the contents of the message?" and she freely gave it out, and that's how these guys were able to get to her T-Mobile Sidekick, and her e-mail, and whatnot.

In another example, the IRS just did a security audit under the office of the inspector general and called 100 managers posing as IT people at the IRS, and 35 of those managers freely gave out their password and user name over the telephone.

So, it's a significant threat. A company can spend hundreds of thousands of dollars on firewalls, intrusion detection systems and encryption and other security technologies, but if an attacker can call one trusted person within the company, and that person complies, and if the attacker gets in, then all that money spent on technology is essentially wasted. It's essentially meaningless.

CNN: How much do you trust online banking and the usage of credit cards online?

MITNICK: I trust online banking. You know why? Because if somebody hacks into my account and defrauds my credit card company, or my online bank account, guess who takes the loss? The bank, not me.

CNN: Then what about other transactions? Do you pay bills online or shop online? I'm just curious if Kevin Mitnick is worried about ID theft?

MITNICK: Somebody already stole my identity once and used it to apply for a cell phone account. And it's too bad. I wish they stole my identity 10 years ago when I was a fugitive -- that would have been cool. It was a \$400 bill, and they used my mom's address in Las Vegas when I was living in California under my name. That's really easy, because all you need to steal someone's identity is the Social Security number. It's not really rocket science.

But, I don't have a problem at all using my credit card online. There are attacks that can be done, but it's unlikely that I'll be targeted as an individual. It's more likely the attackers will target the bank. So that way they can get many user names and passwords, and get access to many accounts, rather than just targeting me. I think it's safer to use a credit card over the Internet than it is to go to a Macy's and use it where an employee can simply skim off the card, or go into a bar, or a restaurant where they have your credit card number.

CNN: You've become something of a star, a cult one, at least, even appearing on an episode of "Alias" as a hacker. What do you make of your celebrity?

MITNICK: It's kind of interesting, because I went through a horrific, horrendous experience and became the hacker poster boy, and it had a negative effect on my trip through the criminal justice system. But now that I've turned over a new leaf and people are interested in my skill-set, now the notoriety of my name helps me in my business. Not because of what I did in the past, but because I'm a known entity with my skill-set.

CNN: Do you miss being on the run?

MITNICK: No, no, I don't miss it all. I like my life now. I made some really stupid mistakes in the past as a younger man that I regret. I'm lucky that I've been given a second chance and that I could use these skills to help the community.