

Print

Monday, August 8, 2011 12:07 AM EDT

## Why Do Hackers Find Many U.S. Companies Easy to Hack?

By IB Times Staff Reporter

Why do big companies fall prey to cyberattacks so easily? According to hackers taking part in the DefCon conference – the world's largest hacking convention, held in Las Vegas -- workers at big corporations are poorly trained in security, which makes it "ridiculously easy" for hackers to trick them and reveal key information to plan cyberattacks against them.

At a time when large organizations like Sony Corp. and International Monetary Fund (IMF) have been targeted for massive security breaches, companies could be expected to pay special attention to security. But hackers who took part in a weekend contest during the annual convention last weekend showed just how easy it was, Reuters reported.

Pretending to be an employee of an IT company, one of the contestants successfully persuaded another employee to pass on information about the configuration of her PC. With the help of that information, a hacker can easily decide what would be the suitable malware to carry out the attack.

"For me it was a scary call, because she was so willing to comply," Chris Hadnagy, one of the organizers of the DefCon contest, told Reuters. "A lot of this could facilitate serious attacks if used by the right people."

A group of benevolent hackers organized DefCon to endorse research on security vulnerabilities, as well as to make companies aware of security issues to fix them. The weekend hacking contest was sponsored by "white-hat" hackers to help expose corporate security loopholes and to encourage companies to create awareness about risks of hacking among employees. ("White-hat" hackers help corporations discover vulnerabilities in their systems.)

### A wake-up call for Oracle

"Oracle was wiped," said Hadnagy, co-author of the book "Social Engineering: The Art of Human Hacking." Employees at Oracle -- one of the world's largest software makers -- gave away the most revealing data, he said.

Apart from Oracle, other companies that were also targeted, included Apple, AT&T, ConAgra Foods, Delta Air Lines, Symantec, Sysco, United Continental Holdings, United Airlines and Verizon Communications.

According to security experts, hackers frequently use "social engineering" to make people hand over information or to download malicious software. In social engineering, hackers send a "spear phishing" e-mail to people pretending to be a friend. The e-mail asks the recipient to open a tainted file or visit a malicious Web site.

Over the past year, numerous hacking activities by hacker groups like LulzSec and Anonymous have been reported. Many organizations such as U.S. defense contractors, the IMF, EMC Corp.'s RSA Security division, Sony, NASA, Arizona Police and government agencies across the world had been targeted.

Information that the contestants managed to obtain from their targets related to data security and backup systems, wireless network use and the names of on-site security providers.

**Must Read: [Top 5 U.S. Government Websites Hacked in 2011](#)**

**Must Read: [AntiSec Claims Revenge by Hacking Websites of US Police Agencies](#)**