

## Hackers: Social networking sites flawed

**AP** Associated Press

By JORDAN ROBERTSON, AP Technology Writer

Fri Aug 3, 11:03 PM ET

Social networking Web sites such as MySpace.com are increasingly juicy targets for computer hackers, who are demonstrating a pair of vulnerabilities they claim expose sensitive personal information and could be exploited by online criminals.

The flaws are being demonstrated this week at the Black Hat and Defcon hacker conferences, which draw thousands of people to Las Vegas each year for five days of training and demonstrations of the latest exploits.

Black Hat, the more genteel of the two events with heavy industry sponsorship and big admission fees, ended Thursday with some 4,000 attendees. Defcon, larger and more roguish, started smoothly Friday, without any of the registration problems that irked fire officials last year and caused lengthy delays. Organizers said more than 6,800 people attended the first day, with more expected Saturday.

There was a moment of drama in the afternoon when organizers received a tip that an undercover NBC producer was covertly filming some of the sessions. The woman was identified during one of the presentations, and she hustled away from the convention site without comment.

An NBC spokeswoman said the network doesn't comment on its newsgathering practices. Defcon organizers said NBC had been offered press credentials but declined.

Infiltrating password-protected social networking sites has been an increasingly fruitful area of study for hobbyists and professional computer security researchers.

One hacker, Rick Deacon, a 21-year-old network administrator from Beachwood, Ohio, says he's discovered a so-called "zero-day" flaw — or a problem that hasn't been patched yet — in MySpace that allows intruders to commandeer personal Web pages and possibly inject malicious code.

Deacon is scheduled to present his findings Sunday. So far, it only affects older versions of the Firefox Web browser and does not affect Internet Explorer, he said.

The attack uses a so-called "cross-site scripting" vulnerability, a common type of flaw found in Web applications that involves injecting code onto someone else's Web page.

The vulnerability could not be independently verified, but experts said these types of attacks are a particular problem for social networking sites, where it's difficult to police the content of the millions of posts each day.

Deacon said the flaw he discovered requires that a user click on a link that leads to a Web page where the computer's "cookie" information is stolen. Deacon said he discovered the problem several months ago along with several other researchers and alerted MySpace, but the company didn't fix the problem.

"Facebook and MySpace both patch things that they find, but it's like a sandbox," Deacon said. "There's so much. And there are probably hundreds more cross-site scripting vulnerabilities there. There's no way they can find them all."

A MySpace spokeswoman declined to comment specifically about Deacon's presentation. The company said in a statement that "it's our responsibility to have the most responsive, solely dedicated 24-7 safety and security team, and we do."

In a separate demonstration, Robert Graham, chief executive of Atlanta-based Errata Security, showed a program for snooping on the computers on public wireless networks to steal the "cookie" information and hijack e-mail accounts and personal Web pages on social networks.

In his Black Hat presentation, he took over the e-mail account of an audience member using Google Inc.'s Gmail service. Graham said his program demonstrates the vulnerability of public wireless connections.

"Everyone has gotten into their minds that passwords over WiFi are toxic, so let's fix that, and they have," Graham said. "What I'm saying is that everything else is just as toxic."

Graham's demonstration would not have worked if the audience member had been using the encrypted version of Gmail.

Google declined to comment specifically on the presentation but said the company is expanding its capacity to enable automatic encryption for all Gmail users.

---

Copyright © 2007 The Associated Press. All rights reserved. The information contained in the AP News report may not be published, broadcast, rewritten or redistributed without the prior written authority of The Associated Press.

Copyright © 2007 Yahoo! Inc. All rights reserved.

[Questions or Comments](#)

[Privacy Policy](#) - [Terms of Service](#) - [Copyright/IP Policy](#) - [Ad Feedback](#)