

Cyber hackers infiltrate ORNL

Spokesman: About 12,000 letters sent to potential victims

By [Frank Munger \(Contact\)](#)

Friday, December 7, 2007

Related information

- [ORNL sets up Web site for potential victims](#)

STORY TOOLS

- [E-mail story](#)
- [Comments](#)
- [iPod friendly](#)
- [Printer friendly](#)

More Local News

- [Speeding motorist killed in early morning I-40 crash](#)
- [Two-alarm blaze damages Jim Gray art gallery](#)
- [KPD releases name of man fatally shot](#)

Share and Enjoy [\[?\]](#)



Get Reprints

 [Want to use this article? Click here for options!](#)

OAK RIDGE - Oak Ridge National Laboratory was the target of a "sophisticated cyber attack" that potentially gave hackers access to the personal information of thousands of visitors to the lab from 1990 to 2004, the laboratory confirmed Thursday.

ORNL Director Thom Mason informed lab staff members of the problem earlier this week and said the lab would attempt to notify "as many persons as possible" whose personal information may have been stolen.

Lab spokesman Billy Stair said Thursday that about 12,000 letters were sent to potential victims.

Mason outlined the general aspects of the attack, which included a number of "phishing" e-mails sent to staff members, but he concluded the note by saying: "Because of the sensitive nature of this event, the laboratory will be unable for some period to discuss further details until we better understand the full nature of this attack."

Phishing is the practice of sending official-looking e-mail to extract information from victims who believe them to be from legitimate institutions such as banks. In ORNL's case, some of the e-mail mimicked notices for scientific

conferences and complaints filed with federal agencies, such as the Federal Trade Commission and the Equal Employment Opportunity Commission.

Mason told staffers that the attack appeared to be part of a "coordinated attempt to gain access to computer networks at numerous laboratories and other institutions across the country." He said ORNL's cyber security team has been working nights and weekends to try to understand the nature of the attack.

A spokesman at Los Alamos National Laboratory, a weapons design laboratory in New Mexico, confirmed Thursday afternoon that LANL also was attacked by hackers.

Kevin Roark of Los Alamos would not discuss the hacking except to say that it occurred on unclassified systems and was "significant and sophisticated." He said Los Alamos employees were notified Nov. 9.

The first potential "corruption" at ORNL occurred Oct. 29, lab officials said.

"Our review to date has shown that while every security system at ORNL was in place and in compliance, the hackers potentially succeeded in gaining access to one of the laboratory's nonclassified databases that contained personal information of visitors to the laboratory between 1990 and 2004," Mason said. "At this point we have determined that the thieves made approximately 1,100 attempts to steal data with a very sophisticated strategy that involved sending staff a total of seven phishing e-mails, all of which at first glance appeared legitimate."

Investigators believe that 11 staff members opened the attachment, enabling hackers to "infiltrate the system and remove data," he said.

Reconstructing the event will likely take weeks, if not longer, to complete, the ORNL director said.

According to Mason, the personal information potentially vulnerable would be names, dates of birth and Social Security numbers of lab visitors. He said there's no evidence at this time that any of the accessed personal information has been used.

Visitors include scientists, university officials, industrial and business representatives, as well as members of the media and many others. The personal information must be submitted in order to get security clearance at the federal lab.

Stair said the ORNL employees who opened attachments on phishing e-mail would be involved "in discussions" to better understand what happened and how to avoid it in the future. He did not say if any punishment was involved.

Mason said, "While our hope is that no one would fall for these kinds of tricks from hackers, we believe there is an ongoing benefit to re-emphasizing staff awareness about cyber security issues. We must not click on e-mail attachments if we are not absolutely sure who the e-mail is from."

A federal audit earlier this year criticized ORNL for not taking sufficient steps to protect the personal information of its employees. The report by the Department of Energy's Office of Inspector General said the lab had been slow in responding to some recommendations, such as installing encryption capabilities on all mobile devices.

Senior writer Frank Munger may be reached at 342-6329.