



Introducing *Mobile Alerts*

✓ Sign Up Today!
COMPUTERWORLD

COMPUTERWORLD
Security



Print Article



Close Window

Study: IRS security vulnerable to social engineering

Grant Gross

August 03, 2007 (IDG News Service) The Internal Revenue Service computer network is vulnerable to social-engineering hacks, with 60% of employees changing their computer passwords when requested by phone callers posing as help desk workers, according to a government auditor.

The IRS employees fell for the ruse even though the Treasury Inspector General for Tax Administration Office has run similar tests with IRS employees two other times since August 2001.

Sixty-one of 102 IRS employees and contractors contacted in March and April agreed to change their passwords to ones requested by callers from TIGTA, posing as IRS help-desk workers.

In the last test, only eight of the 102 employees contacted IRS authorities about the social-engineering attempt.

Seventy-one percent of employees fell for a similar trick in August 2001, but only 35% fell for it in December 2004. TIGTA called the recent results "alarming" in a report ([PDF format](#)) released Friday.

While IRS officials have said there's never been a successful outside attempt to breach agency computers and steal taxpayer data, the social-engineering vulnerabilities raise concerns, the report said.

"This is especially disturbing because the IRS has taken many steps to raise employee awareness of the importance of protecting their computers and passwords," Treasury Inspector General J. Russell George said in a statement. "All the sophisticated encryption and other security mechanisms available will not protect the sensitive taxpayer data on IRS computers until employees get the message loud and clear that they must, at a minimum, protect their passwords."

Asked why they changed their passwords, 21 of the IRS workers said the scenario the caller presented sounded legitimate. Ten employees said they believed that changing their passwords is not the same as disclosing their passwords, which they know is against the rules. Eight employees know the rules but changed their passwords anyway, according to the TIGTA report.

Of the 41 who refused to change their password, 20 said training, e-mail advisories or meetings reinforced the need to protect their passwords, and 17 said they didn't believe the scenario or couldn't verify the caller.

YOU COULD RUN
YOUR LAN TO TOKYO?



Asked why the numbers of disclosures increased from 2004, TIGTA spokeswoman Bonnie Heald said she didn't know. "That's a good question to ask IRS," she said. "IRS has tried to work really hard to raise security awareness."

An IRS spokesman said he didn't think the agency would comment on the report.

TIGTA made recommendations to the IRS, including continued security awareness training and internal social-engineering tests. The agency has agreed with the recommendations, the TIGTA report said.