While Progress Has Been Made, Managers and Employees Are Still Susceptible to Social Engineering Techniques

March 2005

Reference Number: 2005-20-042

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

March 15, 2005

MEMORANDUM FOR CHIEF, MISSION ASSURANCE AND SECURITY SERVICES

Pamela J. Gardiner

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – While Progress Has Been Made, Managers and Employees Are Still Susceptible to Social Engineering Techniques (Audit # 200420035)

This report presents the results of our review to evaluate the susceptibility of Internal Revenue Service (IRS) employees to social engineering techniques for obtaining user account and password information.

In summary, the IRS has successfully completed significant efforts in securing its computer network perimeters from external cyber threats. Because hackers are unable to gain access through these Internet gateways into the IRS, they are likely to seek other ways to gain access to IRS systems and, ultimately, taxpayer data. One of the most common tactics is to convince an organization's employees to reveal their passwords. Along with user account names, passwords are needed to identify and authenticate employees before allowing them access to systems and data.

The IRS has adequate computer security policies and procedures which require employees to protect passwords on IRS computer systems. The IRS requires managers and employees to acknowledge these rules when they are given access to a system and annually thereafter. In addition, the rules are publicized on the Office of Mission Assurance and Security Services (MA&SS) internal web site and during its IRS-wide Computer Security Awareness Week. While these efforts are noteworthy, our tests showed some managers and employees still do not understand the rudimentary computer security practices of protecting their passwords.

We placed telephone calls to 100 managers and employees and posed as Information Technology helpdesk personnel seeking assistance to correct a network problem. Under this scenario, we asked the employees to provide their network login name and temporarily change their password to one we suggested. We were able to convince 35 managers and employees to provide us their user account names and change their

passwords. Using our test scenario, a hacker or disgruntled employee could obtain usernames and passwords to gain unauthorized access to the IRS systems.

Our audit results represented about a 50 percent improvement over a similar test we conducted in August 2001; however, we believe additional security awareness and emphasis are needed to reinforce security responsibilities of IRS employees. For example, the Chief, MA&SS, took aggressive and responsive measures to alert IRS employees of the risks associated with social engineering after being advised of our results. We recommended the Chief, MA&SS, continue security awareness efforts by periodically reminding managers and employees of social engineering risks and providing examples and scenarios that show how hackers can use social engineering tactics to gain access to IRS systems.

Management's Response: The Chief, MA&SS, concurred with our finding and recommendation. The topic of social engineering will be incorporated into the IRS mandatory annual Online Security Awareness Training, which will include examples and scenarios of tactics used to gain access to IRS systems. In addition, the Information Technology Security Program Office will issue periodic reminders in the form of an all-employee notice that will be included with employees' Earnings and Leave statements and an article in the MA&SS newsletter. Management's complete response to the draft report is included as Appendix IV.

Copies of this report are also being sent to the IRS managers affected by the report recommendation. Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Background

The Internal Revenue Service (IRS) annually processes over 222 million tax returns which are converted into electronic records on various IRS systems. This information is protected by law and considered sensitive. Maintaining this type of information could make the IRS a target for computer hackers.

In recent years, the IRS has successfully completed significant efforts in securing its computer network perimeters from external cyber threats. Because hackers are unable to gain access through these Internet gateways into the IRS, they are likely to seek other ways to gain access to IRS systems and, ultimately, taxpayer data.

One such method is social engineering, which involves exploiting the human aspect of computer security for the purpose of gaining insider information about an organization's computer resources. One of the most common tactics is to convince an organization's employees to reveal their passwords. Along with user account names, passwords are needed to identify and authenticate employees before allowing them access to systems and data.

In August 2001, with the assistance of a contractor, we conducted social engineering tests on IRS employees as part of our penetration testing efforts. We placed calls to 100 IRS employees, asking them to change their password to one we suggested, and found 71 employees were willing to accommodate our requests.[1]

This review was conducted from our office in Walnut Creek, California, in December 2004. The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[1] *Management Advisory Report: Network Penetration Study of Internal Revenue Service Systems* (Reference Number 2002-20-057, dated March 2002).

Employees Were Persuaded to Provide Their Network Usernames and Change Their Passwords

The IRS has adequate password policies and procedures. Managers and employees are not to share their passwords with others or reveal them to anyone, regardless of his or her position in or outside the IRS, and are not to accept passwords that are not delivered in a sealed envelope. Password protection allows the IRS to maintain its need to know restriction to IRS computer resources and taxpayer data.

To support password security awareness, the IRS requires all managers and employees to acknowledge these rules prior to obtaining access to any IRS system. Managers and employees must also recertify annually that they are aware of their security responsibilities.

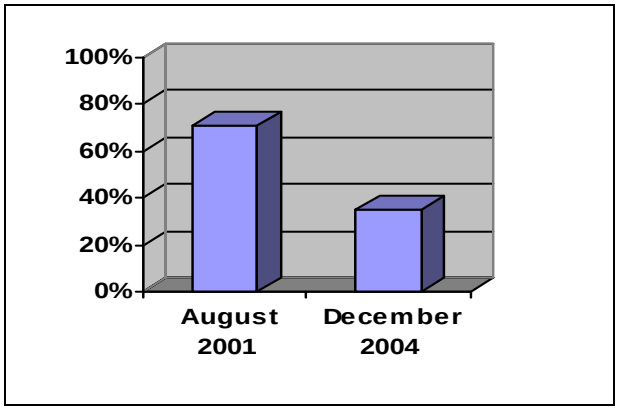
In addition, the Office of Mission Assurance and Security Services (MA&SS)[2] has posted these requirements on its internal web site, created a monthly security newsletter entitled the "Security Sentinel," which contains significant information on computer security, and established an IRS-wide Computer Security Awareness Week, which was held from November 29 to December 3, 2004.

While these awareness efforts are notable, some managers and employees are still susceptible to social engineering techniques. Similar to our tests in 2001, we placed telephone calls to 100 IRS employees, including managers. We posed as Information Technology (IT) helpdesk personnel who were seeking assistance to correct a network problem. Under this scenario, we asked employees to provide their network logon name and temporarily change their password to one we suggested.

We were able to convince 35 managers and employees to provide us their username and to change their password. While our results represented about a 50 percent improvement over the previous test conducted in 2001 (see Figure 1), the noncompliance rate suggests additional emphasis or awareness is needed.

[2] The mission of this office is to ensure the IRS has policies, plans, and procedures in place that will support the continuation of the IRS' business processes under all circumstances and the protection of its employees and other assets (i.e., revenue, data, and facilities).

Figure 1: Percentage of IRS Employees Willing to Change Passwords



Source: Treasury Inspector General for Tax Administration (TIGTA) reviews conducted in 2001 and 2004.

With an employee's user account name and password, a hacker could gain access to that employee's access privileges, though the IRS' strong systemic perimeter controls lessen this risk. Even more significant, a disgruntled employee could use the same social engineering tactics and obtain another employee's username and password. With some knowledge of IRS systems and applications, this disgruntled employee could more easily gain unauthorized access to IRS data as well as damage information on IRS systems.

The 35 managers and employees who were willing to change their password gave several reasons why they were willing to accommodate our request.

- They were not aware of social engineering tactics as well as the security requirements to protect their passwords.
- They were willing to assist in any way possible once we identified ourselves as the IT helpdesk.
- They were having network problems and the call seemed legitimate.
- Although they questioned the caller's identity and could not locate the caller's name, which was fictitious, on the IRS' global email address book, they changed their password anyway.

- They were hesitant, but their managers gave them approval to assist us.

Once informed this exercise was a TIGTA test, some managers and employees admitted they knew they were not supposed to share their password with anyone but did so anyway. During and after the test calls, employees contacted the Audit Manager who was supervising the test as well as the IRS Computer Security Incident Response Center (CSIRC) to verify the calls were part of a TIGTA test.

Within 2 days after completing our test, the Chief, MA&SS, issued an all-employee email alert about possible social engineering telephone calls and notified employees to immediately contact the CSIRC if they received these types of calls. One week after completing our calls, the Chief, MA&SS, provided employees more in-depth information on social engineering as part of the weekly all-employee "IRS Headlines" email. These actions illustrate aggressive, responsive measures to our efforts.

Recommendation

The Chief, MA&SS, should:

1. Enhance security awareness efforts by periodically reminding managers and employees of social engineering risks and providing examples and scenarios that show how hackers can use social engineering tactics to gain access to IRS systems.

Management's Response: The Chief, MA&SS, concurred with our recommendation and has incorporated the topic of social engineering into the IRS mandatory annual Online Security Awareness Training, which includes examples and scenarios of tactics used to gain access to IRS systems. In addition, the IT Security Program Office will issue periodic reminders in the form of an all-employee notice that will be included with the employees' Earnings and Leave statements and an article in the MA&SS newsletter.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the susceptibility of Internal Revenue Service (IRS) employees to social engineering techniques for obtaining user account and password information. To accomplish this objective, we:

I. Evaluated the adequacy of IRS security policies and procedures that have been established to guide IRS employees in recognizing and handling social engineering techniques.

- A. Identified IRS policies, procedures, and guidelines on password security.
- B. Researched Federal Government guidelines and industry standards/guidance on social engineering techniques and defenses.

II. Conducted telephone calls to IRS employees posing as an Information Technology helpdesk employee.

- A. Developed a scenario for social engineering tactics using telephone calls. We decided to use a scenario similar to the one used during our previous test conducted, with the assistance of a contractor, in 2001.
- B. Judgmentally selected a sample of 100 IRS employees from a population of 68,083 employees who were outside the Information Technology Services and the Mission Assurance and Security Services organizations and had network access, as of November 2004. The sample of 100 employees was based on ensuring consistency with the previous test conducted in 2001 and allowing completion of the calls within a 1- to 2-day period with the available staffing.
- C. Prior to our calls, notified the Deputy Commissioner for Operations Support of our test and requested assistance in conducting this test spontaneously, so we could obtain a true gauge of employees' understanding of password security.
- D. Executed the telephone calls and documented the results of the review.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Kent Sagara, Audit Manager
Midori Ohno, Lead Auditor
Alan Beber, Senior Auditor
Bret Hunter, Senior Auditor
Louis Lee, Senior Auditor
William Lessa, Senior Auditor
Abraham Millado, Senior Auditor
Stasha Smith, Senior Auditor
Charles Ekholm, Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Chief Information Officer OS:CIO
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Management Controls OS:CFO:AR:M
Audit Liaisons:
    Chief, Mission Assurance and Security Services OS:MA
    Chief Information Officer OS:CIO

Appendix IV

Management's Response to the Draft Report

CHIEF
MISSION ASSURANCE

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

RECEIVED
MAR 08 2005

March 7, 2005

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDIT
(SMALL BUSINESS AND CORPORATE PROGRAMS)

FROM: Daniel Galik D. Galik
Chief, Mission Assurance and Security Services

SUBJECT: Response to Draft Audit Report - While Progress Has Been Made, Managers and Employees Are Still Susceptible to Social Engineering Techniques (Audit # 200420035)

Security at the Internal Revenue Service (IRS) is a top priority. We are pleased that your draft report acknowledges that the IRS has successfully completed significant efforts in securing its computer network perimeters from external cyber threats and has adequate computer security policies and procedures which require employees to protect passwords on IRS computer systems.

The draft report contains one recommendation regarding social engineering, which involves exploiting the human aspect of computer security for the purpose of gaining insider information about an organization's computer resources. We concur with the report recommendation and have attached a detailed response. Per our discussion with the audit team, we have incorporated the topic of social engineering in the IRS mandatory Online Security Awareness Training. In addition, we will be issuing communications as periodic reminders to employees of this important issue.

If you have any questions, please contact me on (202) 622-8910, or Catherine Quade, Associate Director, Audit Activity Management on (202) 283-5801.

Attachment

Management Response to Draft Audit Report – While Progress Has Been Made, Managers and Employees Are Still Susceptible to Social Engineering Techniques (Audit #200420035)

RECOMMENDATION # 1: Enhance security awareness efforts by periodically reminding managers and employees of social engineering risks and providing examples and scenarios that show how hackers can use social engineering tactics to gain access to IRS systems.

CORRECTIVE ACTION TO RECOMMENDATION #1:

The IT Security Program Office, Assurance Programs, Mission Assurance and Security Services (MA&SS), has incorporated the topic of Social Engineering in the IRS mandatory annual Online Security Awareness Training, which includes examples and scenarios of tactics to gain access to IRS systems. In addition, the IT Security Program Office will issue periodic reminders that will include:

-- An all employee notice message that will be included in Leave and Earnings Statements.

-- An article on Social Engineering will be included in the MA&SS Newsletter.

-- A Business Unit News item will be issued on the IR Web directing all employees to the Social Engineering article referenced in the MA&SS Newsletter.

IMPLEMENTATION DATE:

October 1, 2005

RESPONSIBLE OFFICIAL:

IT Security Program Manager, IT Security Program Office, Assurance Programs, OS:MA:AP

Responsible Partner:
Acting Director, IT Security Field Operations, Assurance Programs, OS:MA:AP

CORRECTIVE ACTION MONITORING PLAN: Completion of the mandatory annual Online Security Awareness Training is tracked by employee. Review of Manager Program Plans will be used to monitor the completion of the periodic reminders.