



*Employees Continue to Be Susceptible to
Social Engineering Attempts That Could Be
Used by Hackers*

July 20, 2007

Reference Number: 2007-20-107

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Redaction Legend:

3(d) = Identifying Information - Other Identifying Information of an Individual or Individuals

Phone Number | 202-927-7037

Email Address | Bonnie.Heald@tigta.treas.gov

Web Site | <http://www.tigta.gov>



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

July 20, 2007

MEMORANDUM FOR CHIEF, MISSION ASSURANCE AND SECURITY SERVICES

FROM: *Michael R. Phillips*
Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers
(Audit # 200720029)

This report presents the results of our review to evaluate the susceptibility of Internal Revenue Service (IRS) employees to social engineering¹ attempts that could be used by hackers to gain access to IRS systems. This review is part of our statutory requirements to annually review the adequacy and security of IRS technology.

Impact on the Taxpayer

The IRS has nearly 100,000 employees and contractors who have access to tax return information processed on approximately 240 computer systems and over 1,500 databases. Using social engineering tactics, we determined IRS employees, including managers, are not complying with the rudimentary computer security practices of protecting their passwords. As a result, the IRS is at risk of providing unauthorized persons access to taxpayer data that could be used for identity theft and other fraudulent schemes.

Synopsis

We made 102 telephone calls to IRS employees, including managers and a contractor, and posed as computer support helpdesk representatives. Under this scenario, we asked for each employee's assistance to correct a computer problem and requested that the employee provide his or her username and temporarily change his or her password to one we suggested. We were

¹ A method used to circumvent existing computer security controls by exploiting the human element to obtain sensitive information that can be used to access computer resources and data.



Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers

able to convince 61 (60 percent) of the 102 employees to comply with our requests. As part of the audit, we also evaluated whether employees contacted appropriate offices to report or validate our test calls. Only 8 of the 102 employees in our sample contacted either the audit team, the Treasury Inspector General for Tax Administration Office of Investigations, or the IRS computer security organization to validate our test as being part of an official Treasury Inspector General for Tax Administration audit.

The above conditions were particularly alarming because we had conducted similar social engineering test telephone calls in August 2001 and December 2004.² Our 2001 and 2004 test calls yielded 71 percent and 35 percent noncompliance rates, respectively. In response to these two prior audits, the IRS took corrective actions to raise awareness of password protection requirements and social engineering attempts. However, the corrective actions have not been effective. Based on the results of this audit, we conclude employees either do not fully understand security requirements for password protection or do not place a sufficiently high priority on protecting taxpayer data in their day-to-day work. To better understand employee behavior, we asked the employees in our sample why they did not comply with IRS password security requirements. Some of the notable reasons given were that the employee thought the scenario sounded legitimate and believable, did not think changing his or her password was the same as disclosing the password, or had experienced past computer problems.

When employees are susceptible to social engineering attempts, the IRS is at risk of providing unauthorized persons access to computer resources and taxpayer data. In addition, when attempts at social engineering are not reported to appropriate personnel, the IRS cannot investigate incidents and take action to minimize the effect of a security breach.

Recommendations

The Chief, Mission Assurance and Security Services, should continue security awareness activities to remind employees of the potential for social engineering attempts and the need to report these incidents to the IRS computer security organization, conduct internal social engineering tests on a periodic basis to increase employees' security awareness and the need to protect usernames and passwords, and coordinate with business units to emphasize the need to discipline employees for security violations resulting from negligence or carelessness.

² *Management Advisory Report: Network Penetration Study of Internal Revenue Service Systems* (Reference Number 2002-20-057, dated March 2002) and *While Progress Has Been Made, Managers and Employees Are Still Susceptible to Social Engineering Techniques* (Reference Number 2005-20-042, dated March 2005).



Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers

Response

IRS management agreed with our recommendations. The Mission Assurance and Security Services organization will continue to deliver social engineering messages and use results from a social engineering survey to remind employees of the potential for social engineering attempts and the need to report these incidents to the IRS Computer Security Incident Response Center. Also, the Mission Assurance and Security Services organization will conduct at least one internal social engineering test during Fiscal Year 2008 to increase employees' security awareness and the need to protect usernames and passwords. The test will be robust and statistically diverse, surveying thousands of IRS employees. The IRS will communicate the results of the tests to business units to increase awareness. Additionally, a revised Penalty Guide has been developed and is currently being negotiated with the National Treasury Employees Union. When the Guide is published, the Mission Assurance and Security Services organization will emphasize to the business units the need to implement the new guidance. Management's complete response to the draft report is included as Appendix V.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. 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.



Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers

Table of Contents

BackgroundPage 1

Results of ReviewPage 3

 Employees Continue to Struggle With Complying With the Basic Security Requirements of Protecting Their Passwords and Reporting Possible Security IncidentsPage 3

Recommendation 1:.....Page 5

Recommendations 2 and 3: Page 6

Appendices

 Appendix I – Detailed Objective, Scope, and MethodologyPage 7

 Appendix II – Major Contributors to This ReportPage 8

 Appendix III – Report Distribution ListPage 9

 Appendix IV – Results From Test CallsPage 10

 Appendix V – Management’s Response to the Draft ReportPage 13



Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers

Abbreviations

IRS	Internal Revenue Service
TIGTA	Treasury Inspector General for Tax Administration



Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers

Background

During an interview with the National Public Radio on April 7, 2007, regarding the Treasury Inspector General for Tax Administration (TIGTA) audit report¹ on the loss of computers containing sensitive taxpayer data, the Internal Revenue Service (IRS) Commissioner stated, “Every day, there are attempts to get into our databases, and there has never been a penetration of the IRS databases from the outside.” In recent years, TIGTA Office of Audit penetration tests have confirmed that the IRS has secured its computer network perimeters from external cyber threats.

As more attacks are blocked at an organization’s computer network perimeters, hackers have turned to alternative methods to break into computer systems and steal sensitive data. One method is social engineering, which is used to circumvent existing computer security controls by exploiting the human element to obtain sensitive information that can be used to access computer resources and data. A typical social engineering tactic involves a hacker posing as an internal employee, such as a computer support person, and calling employees to convince them to share critical information about (1) the organization, computer system, or infrastructure or (2) their usernames and passwords.

We have previously conducted two tests to evaluate employee susceptibility to social engineering attempts. In August 2001, we found 71 of 100 employees were willing to provide us with their usernames and change their passwords to one we suggested.² In December 2004, we used the same methodology and found a 50 percent improvement, with only 35 of 100 employees willing to provide their usernames and change their passwords.³ From both audits, we made recommendations to improve employee training on social engineering attempts and issue periodic awareness publications on the dangers of social engineering.

Exposing sensitive data unnecessarily can lead to potential identity theft and/or other fraudulent schemes. Identity theft refers to a crime in which someone wrongfully obtains and uses another person’s personal data in some way that involves fraud or deception, typically for financial or economic gain. According to the Federal Bureau of Investigation, identity theft is one of the fastest growing white-collar crimes in the United States. The Department of Commerce estimates that more than 50 million identities were compromised in Calendar Year 2005. The

¹ *The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Electronic Media Devices* (Reference Number 2007-20-048, dated March 23, 2007).

² *Management Advisory Report: Network Penetration Study of Internal Revenue Service Systems* (Reference Number 2002-20-057, dated March 2002).

³ *While Progress Has Been Made, Managers and Employees Are Still Susceptible to Social Engineering Techniques* (Reference Number 2005-20-042, dated March 2005).



Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers

challenges for the IRS in protecting against identity theft are the amount and sensitivity of the information it processes and the sheer size of the organization, which employs nearly 100,000 employees and contractors who have access to tax return information processed on approximately 240 computer systems and over 1,500 databases.

This review is part of our statutory requirements to annually review the adequacy and security of IRS technology. We also recognized the enormous and political risk of exposing sensitive taxpayer information, educating employees on protecting taxpayer data, and following up to ensure security solutions are working as intended. This review was performed from our office in Walnut Creek, California, and in the Office of Mission Assurance and Security Services in Lanham, Maryland, during the period March through April 2007. 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.



Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers

Results of Review

Employees Continue to Struggle With Complying With the Basic Security Requirements of Protecting Their Passwords and Reporting Possible Security Incidents

Password protection is one of the basic and rudimentary computer security practices for organizations, and the IRS has adequate password policies and procedures. Managers and employees are not to reveal or share their passwords with anyone, regardless of his or her position inside or outside of the IRS. This includes, but is not limited to, the employee's manager, helpdesk staff, system administrators, and security personnel. Additionally, employees are not to accept passwords that are not delivered securely. Password protection allows the IRS to limit access to its computer resources and taxpayer data to persons who need it to accomplish their official duties. To support password security awareness, the IRS requires all managers and employees to acknowledge these rules prior to obtaining access to any IRS computer systems and to annually recertify they are aware of their responsibilities.

The IRS has posted these requirements and password security policies on its internal web site. The web site also has a document that describes social engineering and provides examples of social engineering attempts, specifically mentioning the use of telephone calls to conduct this type of attack. The document uses an example of a caller pretending to be someone needing assistance and attempting to get the employee to reveal his or her logon information and change his or her password to one the caller suggests.

While these awareness efforts are notable, managers and employees continue to be susceptible to social engineering attempts. We made 102 telephone calls to employees, including managers and a contractor, and posed as Modernization and Information Technology Services organization helpdesk personnel who were seeking assistance to correct a network problem. This is the same scenario we used in our prior two social engineering tests. Under this scenario, we asked each employee to provide his or her username and temporarily change his or her password to one we suggested. We were able to convince 61 (60 percent) of the 102 employees to comply with our requests, even though doing so violated the IRS security policy and procedures. Appendix IV provides further details about our sample and audit results.

We limited our sample to 102 employees because we had to make the telephone calls quickly before our tests were publicized throughout the IRS. Due to the sample size, we were unable to project our results throughout the IRS. However, we believe our sample was sufficient to demonstrate that IRS employees continue to be susceptible to social engineering attempts and



Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers

that employees do not provide sufficient emphasis to the security of taxpayer data in their day-to-day activities.

To better understand employee behavior, after informing the employees and managers in our sample that the calls were part of a TIGTA social engineering audit, we asked them why they did not comply with IRS password security requirements. The 61 noncompliant employees provided the following reasons:

- The scenario sounded legitimate and believable (21 employees).
- The employee believed changing his or her password was not the same as disclosing the password, which he or she knew was against the rules (10 employees).
- The employee knew the rules but changed his or her password anyway (8 employees).
- The employee was having or had previously had computer problems (7 employees).
- The employee had a lack of training or did not know the rules to protect his or her password (4 employees).
- No reason was provided (11 employees).

The 41 employees who complied with the password security requirements provided the following reasons for not providing their passwords:

- Awareness training, email advisories, or group meetings reinforced the need for protecting his or her username and/or password (20 employees).
- The employee did not believe the scenario or could not verify the caller (17 employees).
- No reason was cited (4 employees).

As part of this audit, we also evaluated whether IRS employees contacted appropriate personnel after we had informed them the calls were part of a TIGTA audit and ended the calls. Potential security breaches, including attempted and actual security breaches, should be forwarded to the IRS computer security organization for notification and further evaluation. Information on these incidents allows the computer security organization to minimize the impact of a security breach and determine whether the IRS is being attacked on various fronts or the incidents are isolated. The IRS computer security organization received contact from only one IRS employee who reported that a call came from the TIGTA Office of Audit as part of the social engineering test and he or she was concerned about the test.

In addition, the following contacts were made by IRS employees:

- The manager of the audit team received telephone calls from three employees to verify the calls were part of an official TIGTA audit.



Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers

- The TIGTA Office of Investigations received contacts from four employees who had been called as part of this test.

The IRS cannot react swiftly to thwart social engineering attempts and other potential security breaches when employees do not notify appropriate authorities. While our calls were part of an official TIGTA audit, hackers could include a reference to a nonexistent TIGTA audit in an attempt to divert attention from their social engineering attempts, particularly if an employee questions the call.

The above conditions were particularly alarming because we had conducted similar social engineering test telephone calls in August 2001 and December 2004. In the respective management responses to those audits, the IRS stated it:

- Would update its security awareness program to include training on computer intrusions and unauthorized access and use existing media, such as the annual security training and security awareness week, to communicate IRS security standards on password protection procedures.
- Had incorporated the topic of social engineering into its mandatory annual Online Security Awareness Training, which included examples and scenarios of attempts used to gain access to IRS systems. In addition, the IRS stated periodic reminders would be issued in the forms of (1) all-employee notices that would be included with employees' Earnings and Leave statements and (2) articles in the computer security newsletter.

These corrective actions were completed but have not been effective. Based on our results, we conclude employees either do not fully understand security requirements for password protection or do not place a high priority on protecting taxpayer data in their day-to-day work.

When employees are susceptible to social engineering attempts, the IRS is at risk of providing unauthorized persons access to computer resources and taxpayer data that could be used for identity theft and other fraudulent purposes. In addition, when attempts at social engineering are not reported to appropriate personnel, the IRS cannot investigate incidents and take action to minimize the effect of a security breach.

Recommendations

The Chief, Mission Assurance and Security Services, should:

Recommendation 1: Continue security awareness activities to remind employees of the potential for social engineering attempts and the need to report these incidents to the IRS Computer Security Incident Response Center in the Office of Mission Assurance and Security Services.

Management's Response: The Chief, Mission Assurance and Security Services, agreed with our recommendation and will continue to deliver social engineering



Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers

messages as specified in the 2007 Information Security Awareness Plan. In addition, the Mission Assurance and Security Services organization has worked with the Communications and Liaison organization to conduct a survey on social engineering to assess the knowledge base of IRS personnel. The results of this survey are being used to tailor future communications efforts to remind employees of the potential for social engineering attempts and the need to report these incidents to the IRS Computer Security Incident Response Center.

Recommendation 2: Conduct internal social engineering tests on a periodic basis to increase employees' security awareness and the need to protect usernames and passwords. The results of these tests should be provided to all IRS employees.

Management's Response: The Chief, Mission Assurance and Security Services, agreed with our recommendation and will conduct at least one internal social engineering test during Fiscal Year 2008, using lessons learned from TIGTA tests, to increase employees' security awareness and the need to protect usernames and passwords. The test sample will be robust and statistically diverse, surveying thousands of IRS employees. The results of these tests will be communicated to business units to increase awareness.

Recommendation 3: Coordinate with business units to emphasize the need to discipline employees for security violations resulting from negligence or carelessness.

Management's Response: The Chief, Mission Assurance and Security Services, agreed with our recommendation. A revised Penalty Guide has been developed and is currently being negotiated with the National Treasury Employees Union. When the Penalty Guide is published, the Mission Assurance and Security Services organization will emphasize to the business units through various communications the need to implement the new guidance.



Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the susceptibility of IRS employees to social engineering¹ attempts that could be used by hackers to gain access to IRS systems. To accomplish this objective, we:

- I. Evaluated the adequacy of IRS security policies and procedures that have been established to guide employees in recognizing and handling social engineering attempts.
- II. Informed the Deputy Commissioner for Services and Enforcement; the Deputy Commissioner for Operations Support; the Chief, Mission Assurance and Security Services; and the TIGTA Office of Investigations of our social engineering tests on the day we made the telephone calls.
- III. Made telephone calls to IRS employees and managers posing as a Modernization and Information Technology Services organization helpdesk employee.
 - A. Developed a scenario for social engineering attempts using telephone calls. We decided to use a scenario similar to the one we had used during our previous tests in 2001 and 2004.
 - B. Judgmentally selected a sample of 102 IRS employees, including managers and a contractor, from a population of 95,858 employees who were outside of the Modernization and Information Technology Services and the Mission Assurance and Security Services organizations as of January 19, 2007. We used a judgmental sample because we were not projecting the audit results and needed to complete the telephone calls before our test was publicized throughout the IRS.
 - C. Made 102 telephone calls in 1 day to the sample of employees.
- IV. Reviewed the planned corrective actions from our two previous social engineering reviews to determine whether the IRS' corrective actions had been implemented.²

¹ A method used to circumvent existing computer security controls by exploiting the human element to obtain sensitive information that can be used to access computer resources and data.

² *Management Advisory Report: Network Penetration Study of Internal Revenue Service Systems* (Reference Number 2002-20-057, dated March 2002) and *While Progress Has Been Made, Managers and Employees Are Still Susceptible to Social Engineering Techniques* (Reference Number 2005-20-042, dated March 2005).



Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Kent Sagara, Audit Manager
Midori Ohno, Lead Auditor
Richard Borst, Senior Auditor
Cari Fogle, Senior Auditor
Michael Garcia, Senior Auditor
Allen Gray, Senior Auditor
Bret Hunter, Senior Auditor
Jody Kitazono, Senior Auditor
Louis Lee, Senior Auditor
Abraham Millado, Senior Auditor
Beverly Tamanaha, Senior Auditor
Louis Zullo, Senior Auditor



Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers

Appendix III

Report Distribution List

Acting Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Commissioner for Services and Enforcement SE
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 Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
 Chief Information Officer OS:CIO
 Chief, Mission Assurance and Security Services OS:MA



Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers

Appendix IV

Results From Test Calls

For further perspective on our test results, we gathered additional information on the telephone calls we made.

Figure 1 presents our results from the 102 IRS employees in our sample by IRS business unit.

Figure 1: Test Call Results by IRS Business Unit

Business Unit	Number of Employees	Changed Password
Agency-Wide Shared Services	3	2
Communications and Liaison	1	0
Criminal Investigation	2	1
Human Capital Office	4	2
Large and Mid-Size Business	4	4
National Taxpayer Advocate	7	3
Office of Appeals	4	2
Office of Chief Counsel	2	0
Small Business/Self-Employed	27	15
Tax Exempt and Government Entities	3	2
Wage and Investment	45	30
TOTALS	102	61

Source: TIGTA analysis of the IRS business units included in the audit test.



Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers

Figure 2 presents our results by IRS locations of the 102 employees.

Figure 2: Test Call Results by IRS Location

Location	Number of Employees	Changed Password
Western (California, Colorado, Nevada, Oregon, Utah, Washington, Wyoming)	25	18
South (Florida, Georgia, Kentucky, Louisiana, Tennessee, and Texas)	41	22
Midwest (Indiana, Kansas, Michigan, Missouri, Ohio, South Dakota)	15	7
East (Connecticut, Delaware, Massachusetts, Maryland, New Jersey, New York, Pennsylvania, Washington, D.C., and West Virginia)	21	14
TOTALS	102	61

Source: TIGTA analysis of the IRS locations included in the audit test.

Figure 3 presents our results by employee and manager positions, based on the individual's job title. For example, job titles with the words supervisor, supervisory, manager, or branch chief were considered managers.

Figure 3: Test Call Results by Employee and Manager Positions

Position	Number of Employees	Changed Password
Employees ¹	79	45
Managers	23	16
TOTALS	102	61

Source: TIGTA analysis of the IRS positions included in the audit test.

¹ The total number of employees included a contractor.



Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers

Figure 4 presents our results by the grade levels of the 102 IRS employees.

Figure 4: Test Call Results by Grade Levels

Grade Level	Number of Employees	Changed Password
GS-4	3(d)	
GS-5		
GS-6		
GS-7		
GS-8		
GS-9		
GS-10		
GS-11		
GS-12		
GS-13		
GS-14		
GS-15		
Contractor		
TOTALS	102	61

Source: TIGTA analysis of the employee grade levels included in the audit test. GS = General Schedule.



Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers

Appendix V

Management's Response to the Draft Report



CHIEF
MISSION ASSURANCE AND SECURITY SERVICES

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

RECEIVED
JUN 28 2007

June 26, 2007

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

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

SUBJECT: Response to Draft Audit Report – Employees Continue to Be Susceptible to Social Engineering Attempts that Could Be Used by Hackers (Audit #200720029), (I-Trak #2007-25135)

Thank you for the opportunity to review and respond to the referenced draft audit report. The Internal Revenue Service (IRS) takes its security posture very seriously and we recognize the risks associated with exposing sensitive data unnecessarily. We appreciate your report recognizing that recent Treasury Inspector General for Tax Administration audits of penetration tests confirmed that the IRS has secured its computer network perimeter from external cyber threats. We continue to reemphasize computer security practices, including social engineering, to IRS personnel.

We concur with the three report recommendations and have provided detailed corrective action plans in the attachment. If you have any questions, please contact me at (202) 622-8910, or Devon Bryan, Director, Information Technology Security, at (202) 283-7271.

Attachment



Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers

Attachment

Management Response to Draft Audit Report – Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers (Audit # 200720029)

RECOMMENDATION #1:

The Chief, Mission Assurance and Security Services, should continue security awareness activities to remind employees of the potential for social engineering attempts and the need to report these incidents to the IRS Computer Security Incident Response Center in the Office of Mission Assurance and Security Services organization.

CORRECTIVE ACTION TO RECOMMENDATION #1:

Mission Assurance and Security Services (MA&SS) will continue to deliver social engineering messages as specified in the 2007 Information Security Awareness Plan. In addition, MA&SS has worked with Communications & Liaison to conduct a survey on social engineering to assess the knowledge base of IRS personnel. The results of this survey are being used to tailor future communications efforts appropriately to remind employees of the potential for social engineering attempts and the need to report these incidents to the IRS Computer Security Incident Response Center in MA&SS.

IMPLEMENTATION DATE: June 15, 2008

RESPONSIBLE OFFICIAL: Director, IT Security, OS:MA:IT

CORRECTIVE ACTION MONITORING PLAN:

Monthly reports on progress on all corrective actions are provided to the Director IT Security.



Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers

Attachment

RECOMMENDATION #2:

The Chief, Mission Assurance and Security Services, should conduct internal social engineering tests on a periodic basis to increase employees' security awareness and the need to protect usernames and passwords. The results of these tests should be provided to all IRS employees.

CORRECTIVE ACTION TO RECOMMENDATION #2:

Mission Assurance and Security Services will conduct at least one internal social engineering test during the FY 2008, using lessons learned from TIGTA tests, to increase employees' security awareness and the need to protect usernames and passwords. The test sample will be robust and statistically diverse surveying thousands of IRS employees. Reports from these tests will be communicated to business units as part of increased awareness.

IMPLEMENTATION DATE: October 15, 2008

RESPONSIBLE OFFICIAL: Director, IT Security, OS:MA:IT

CORRECTIVE ACTION MONITORING PLAN:

Monthly reports on progress on all corrective actions are provided to the Director IT Security.



Employees Continue to Be Susceptible to Social Engineering Attempts That Could Be Used by Hackers

Attachment

RECOMMENDATION #3:

The Chief, Mission Assurance and Security Services, should coordinate with business units to emphasize the need to discipline employees for security violations resulting from negligence or carelessness.

CORRECTIVE ACTION TO RECOMMENDATION #3:

A revised Penalty Guide has been developed and is currently being negotiated with the National Treasury Employees' Union. As soon as the Penalty Guide is published, Mission Assurance and Security Services shall emphasize to the business units through various communications the need to implement the new guidance.

IMPLEMENTATION DATE: February 15, 2008

RESPONSIBLE OFFICIAL: Director, IT Security, OS:MA:IT

CORRECTIVE ACTION MONITORING PLAN:

Monthly reports on progress on all corrective actions are provided to the Director IT Security.