IDEA GROUP PUBLISHING ITB11412

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This chapter appears in the book, *Managerial Guide for Handling Cyber-Terrorism and Information Warfare* by Lech J. Janczewski and Andrew Colarik © 2005, Idea Group Inc.

Chapter 9

Identity Stealing Attacks

In recent years, several feature films have been produced based on the concept of stealing an identity. As a result of deliberate or accidental changes to personal records, a person can cease to exist on paper, or someone else can acquire a person's identity. These film directors' concepts are not products of their rich imaginations, but are a reflection of reality. Quite often, we read about such accidents happening. Stealing an identity is a favorite step in the preparation of terrorist and cyber-terrorist attacks, and all of us, IT managers in particular, should be vigilant about such possibilities.

Examples of Identity Theft Attacks

Stealing an identity can vary from simple impersonations to elaborate electronic scams. An example of a traditional impersonation occurred during the first half of 2003 when a person of Middle Eastern origin was attending a private airplane pilot program in New Zealand. Towards the end of the training, this person left the country, but someone else arrived at the examination site and pretended to be that person. Fortunately, the fraud was discovered before the examination for the license was over. The impersonator claimed that all he wanted to do was help the stranger get the licence. The case is under considerable investigation at the time of writing this text.

Cases of stealing people's identity via e-mail are quite popular. There is a recent surge in the sending of spam messages that look as though the message comes from a reputable company. It is quite easy to fake the sender's IP address (spoof) in such correspondence, as mentioned in a previous chapter. Typically, these e-mails tell you the following:

- Your account has had some issues.
- New policies and procedures need your authorization.
- You need to participate in some customer satisfaction survey (for a reward).
- We are offering great deals, if you register now.

If you register, you will need to supply some of your personal data, which then can be used to the advantage of the person behind such a scheme. An example of such a scam is presented in Case 9.1. The term *phishing* is used to describes identity theft activities.

Case 9.1: Example of phishing: Westpac Bank

In November 2003, many Westpac Bank customers in New Zealand received an e-mail with the following content:

Dear Westpac Bank Member,

This e-mail was sent by the Westpac server to verify your e-mail address. You must complete this process by clicking on the link below and entering in the small window your Westpac Banking Customer ID and Password. This is done for your protection – because some of our members no longer have access to their e-mail addresses, and we must verify it.

To verify your e-mail address and access your bank account, click on the link below. If nothing happens when you click on the link, copy and paste the link into the address bar of your Web browser.

http://www.westpac.com.nz:ac-YivzaYoco3Kn6oX2tKIv@rk3bcj0tu.Da. rU/?on9Pji4ztg0qAw1

Thank you for using Westpac Bank!

This automatic e-mail sent to: (hubby's email address)
Do not reply to this e-mail.

Oxie (Lyn)

(case continued on the following page)