THE TRUTH ABOUT

IDENTITY THEFT

"Why be me, when I can be you?"

Jim Stickley
Internationally renowned security expert appearing regularly on the *Today* show

Publishing as FT Press
Upper Saddle River, New Jersey 07458

Printed in the United States of America

First Printing August 2008

ISBN-10: 0-7897-3793-0
ISBN-13: 978-0-7897-3793-9

Pearson Education LTD.
Pearson Education Australia PTY, Limited.
Pearson Education Singapore, Pte. Ltd.
Pearson Education North Asia, Ltd.
Pearson Education Canada, Ltd.
Pearson Educatión de Mexico, S.A. de C.V.
Pearson Education—Japan
Pearson Education Malaysia, Pte. Ltd.

Library of Congress Cataloging-in-Publication Data on file.

Publisher
Paul Boger

Associate Publisher
Greg Wiegand

Acquisitions Editor
Rick Kughen

Development Editor
Rick Kughen

Technical Reviewer
"Wild Bill" Stanton

Marketing Coordinator
Judi Taylor

Cover and Interior Designs
Stuart Jackman, Dorling Kindersley

Managing Editor
Kristy Hart

Senior Project Editor
Lori Lyons

Copy Editor
Karen A. Gill

Design Manager
Sandra Schroeder

Compositor
Gloria Schurick

Proofreader
San Dee Phillips

Manufacturing Buyer
Dan Uhrig

Introduction

I have stolen credit cards, hacked social security numbers, robbed banks, and created fake ATMs. I have broken into armed government facilities and have stolen from teenagers. I am an identity thief, but I am no criminal.

In the end, I have found there is little separation between attacking a corporation in New York City and targeting a housewife in Dover, Ohio.

I am an identity thief, but I am no criminal.

Fortunately for all victims involved, I was hired to perform these attacks by corporations testing their security, news agencies investigating security concerns, and other media outlets interested in knowing just how easy it is to commit identity theft. My job is to find security flaws before the real criminals find them.

My job is to find security flaws before the real criminals find them.

This book has been designed to give you the insight that most people experience only after becoming victims of identity theft. Each Truth walks you through a different type of attack, explaining the complete process in a simple and straightforward way.

Like a magician actually revealing what happens behind the curtain, I take you through the attacks to reveal how people at home, work, and on the road become victims. I identify tips on how to protect yourself, your office, and your children from becoming the next identity theft statistics.

Identity thieves can, and often do, use all the attacks against any type of target, regardless of whether they are after you in your home in the Midwest or if they are targeting you in your New York City office. While learning to think like an identity thief, you will begin to look at situations in an entirely new way. You might think twice about that preapproved credit card application that arrived in the mail, and you might keep a closer eye on that pest inspector who has spent just a

little too much time walking around your office. Ultimately, this book opens your eyes to a world most people never knew existed.

There is no doubt that I have had to walk a fine line when performing the attacks that I outline in this book. On one hand, I am hired by organizations to conduct these tests; on the other hand, I am stealing the confidential information of millions of unsuspecting individuals. In the end, the information I steal ends up being far more secure than before I touched it, and the lessons learned have benefited hundreds of thousands of others in their efforts to avoid being the next identity theft victims. Of course, there have been engagements that were flat-out illegal. In those cases, the proper authorities were notified ahead of time, and although the attacks were real and unrehearsed, I had my "get out of jail free" paperwork.

In this day and age, what you don't know is exactly what can hurt you.

In this day and age, what you don't know is exactly what can hurt you. Identity thieves are out there, and their success often comes from innocent mistakes made by others.

TRUTH 5

One man's trash is another man's identity

Through the years, I have broken into numerous banks through hundreds of different attacks. Though each was different, the main objective was often the same: to gain access to the cash or confidential information. I was once approached by a large financial institution that was not only concerned about the security of its physical locations and its network, but also had concerns about the risks associated with upper management. This institution asked that I also investigate whether its management team could be attacked in a way that might allow an identity thief greater access to its organization.

So each afternoon I waited in the parking lot and watched members of the management team get into their vehicle. Then I followed them home. Within a couple of weeks, I had each of their home addresses. Since I had no permission to break into their homes and poke through their personal belongings, I opted for the next best thing: their garbage.

Through the years, I have been amazed at the things you can find in the trash. There is big business for identity thieves in personal garbage. More importantly, when you put your garbage out on the street for trash pickup, it usually becomes open to the public. This means that if I am so inclined, I can take that garbage and bring it home, which is exactly what I did. Each week I would snap on my rubber gloves and go through every item of trash: grocery store shopping lists, sticky notes with phone numbers, a private invitation for a little girl to a friend's birthday party, and much more. As I continued to go through the managers' trash, I was able to compile a list of their service providers: water bill, phone bill, gas and electric, cable, and so on. I could use this information not only to gain access into their lives but, if I wanted, to take over their lives.

I could use this information not only to gain access into their lives but, if I wanted, to take over their lives.

Ultimately, I decided to use the billing information for the bank managers' Internet service providers as an access point for my attack. Using the information I gained from the bills, I contacted the managers and explained that I was from that company. I told them that we were updating our services and that,

for them to continue to have Internet service, they would be required to install updated software. I explained that the software would be arriving within the next week.

Because I was also able to reference their past billing information during the call, the victims never suspected a thing. Within a week, they each received a package in the mail that contained "upgrade software" and instructions. One by one, the managers installed the software.

Of course, the software they had just installed was actually malicious and designed specifically to allow me to access their computer via the Internet from anywhere in the world. Shortly after they installed the software, I was on their computers going through all their files. Within a few short days, I had usernames and passwords to corporate systems and even VPN access, which allowed me to connect directly to the financial institution's internal network.

When I submitted my report to the executives at the organization, they were obviously floored. None of them had ever suspected that I had targeted them at home, even though they had all signed waivers allowing me to do so. They said they were being cautious about emails that were being sent to them, as they were convinced that was how I was going to try to get in; but the idea that I would go through their trash and use that against them had never crossed their minds.

Now, you might be asking yourself what that story has to do with identity theft. Sure, I was able to gain access to that financial institution by attacking its employees at home, but technically the employee was never placed directly at risk, just the employer. In reality, those employees turned out to be far more vulnerable than I would have imagined. However, since I was not hired to test them personally, I just bypassed those opportunities and stayed focused on my primary target: the bank.

If you own a credit card, you are probably used to the clutter of junk mail that comes on behalf of the credit card company. While most of the junk included with your bill is harmless, the issue occurs when the credit card company decides to make it easier for you to spend money. Credit card checks have become a lucrative business for credit card companies. These checks can be used just like regular checks to pay anything from other credit card bills to buying food at the grocery store. Because you can use these checks in situations

where credit cards would not have been accepted, they allow you a new freedom to continue to rack up credit card debt. These checks are often included with numerous other documents that are all stuffed into your monthly credit card statement.

While attacking the bank's management team, I found many of these checks still inside the opened statement envelope, which had been dropped in the trash. All I had to do was take these checks and go on a shopping spree.

There were other identity theft attack opportunities made available to me during these tests. Each bill that I found contained great information. For example, on the cable bill, the victim's name, address, and account number were available. In addition, I could see the total of the current bill, the amount of the previous bill, and if they paid it. Using just this information, I could call the victim, explain that I was from the cable company, and say that we had not received a payment for this month's bill. The victim, of course, would say he had paid it, and I would argue that he may have sent a check, but we had not received it, so it may be lost in the mail. I would explain that, though unfortunate, his service was being turned off and he would have to incur a fee to have it reenabled.

I would then offer the victim the ability to pay the bill via a credit card or check over the phone. I would explain that if his other payment did finally show up, it would be destroyed. Again, it is important to note that mentioning the victim's previous payment amount and when it was received helped lend me credibility. The victim would relent and give his credit card number or checking account number and bank routing number. Once complete, I could've simply taken that information and gone on a buying spree.

There is a simple solution to avoiding this kind of attack: Shred everything. I mean it. Everything! If you are throwing away any paper that contains personal information, shred it first. Shredders come in a few different types, but I highly recommend that you spend a little extra to make sure that it does cross-cut shredding and can shred CDs and credit cards. This type of shredder runs faster and shreds more items at a time, allowing you to spend less time standing in front of it.

Remember: One man's trash truly can be another man's treasure. Unfortunately, one man's treasure might actually be stolen from another man's identity. So start shredding.