Brought to you by

Access Smart™

Giving security to the power of smart

Online Identity Theft Protection FOR DUMMIES®

Power LogOn™ Edition

Understand the risks and costs to companies and individuals

A Reference for the Rest of Us!®

FREE eTips at dummies.com®

Dovell Bonnett

Founder and CEO, Access Smart, LLC
Creator of Power LogOn

Online Identity Theft Protection FOR DUMMIES®

POWER LOGON™ EDITION

by Dovell Bonnett
Founder and CEO, Access Smart, LLC

1807
WILEY
2007

Wiley Publishing, Inc.

Online Identity Theft Protection For Dummies®, Power LogOn™ Edition

Published by
Wiley Publishing, Inc.
111 River Street
Hoboken, NJ 07030-5774

www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. FULFILLMENT OF EACH COUPON OFFER IS THE SOLE RESPONSIBILITY OF THE OFFEROR.

For general information on our other products and services, please contact our Customer Care Department within the U.S. at 800-762-2974, outside the U.S. at 317-572-3993, or fax 317-572-4002.

For technical support, please visit www.wiley.com/techsupport.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

ISBN: 978-0-470-12947-0

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

About the Author

Dovell Bonnett is the Founder and CEO of Access Smart, LLC. He has been creating security solutions for computer users for more than 20 years. He founded Access Smart in order to provide these solutions to consumers as directly and quickly as possible. Dovell's solutions reduce security risks for individual users, small businesses, and large corporations.

His professional experience spans 21 years in engineering, product development, and sales and marketing, with more than 13 years focused specifically on smartcard technology, systems, and applications. Dovell has spent most of his smartcard career translating and integrating technology components into end-user solutions designed to solve business security needs and incorporating multi-applications onto a single credential using both contactless and contact smartcards. He has held positions at National Semiconductor, Siemens (Infineon), Certicom, Motorola, and HID. He is the author of smartcard articles, regularly presents at conferences, and helps companies successfully implement smartcard projects. Dovell has been an active member of the Smart Card Alliance and a contributor to the development of physical access security white papers. He holds dual bachelor's degrees in industrial and electrical engineering from San Jose State University.

Dedication

To my beautiful wife, Marguerite, who has given me unquestionable support in my new endeavor, has listened to me as I gave numerous explanations about smartcards to anyone who would listen, and has tolerated my relentless zeal regarding security.

Author's Acknowledgments

I am deeply grateful to all my colleagues, partners, and friends who have helped me write and edit this book. Their devotion to my desire for protecting people's identities and computer data is what drove me to write this book. I would like to especially thank the following people for their contributions: Nicole Friel, Larry Harris, Don Kasle, Christine Wecker, and Dietrich Wecker.

Publisher's Acknowledgments

We're proud of this book; please send us your comments through our online registration form located at `www.dummies.com/register/`. For information about a custom *Dummies* book for your business or organization, contact `BrandedRights&Licenses@Wiley.com`.

Some of the people who helped bring this book to market include the following:

Acquisitions, Editorial, and Media Development

Senior Project Editor: Zoë Wykes

Development Editor: Colleen Totz Diamond

Business Development Representative: Karen L. Hattan

Editorial Manager: Rev Mengle

Cartoons: Rich Tennant (`www.the5thwave.com`)

Composition Services

Project Coordinator: Kristie Rees

Layout and Graphics: Stephanie D. Jumper, Erin Zeltner

Proofreaders: Charles Spencer

Anniversary Logo Design: Richard Pacifico

Publishing and Editorial for Technology Dummies

Richard Swadley, Vice President and Executive Group Publisher

Andy Cummings, Vice President and Publisher

Mary Bednarek, Executive Acquisitions Director

Mary C. Corder, Editorial Director

Publishing for Consumer Dummies

Diane Graves Steele, Vice President and Publisher

Joyce Pepple, Acquisitions Director

Composition Services

Gerry Fahey, Vice President of Production Services

Debbie Stailey, Director of Composition Services

Table of Contents

Introduction

Identity theft is the fastest growing crime in America. Whether your credit card is being used to make fraudulent purchases or a thief is taking out loans in your name, identity theft is bad news. And it's not just about individuals anymore: Criminals are launching full-scale attacks on all sizes of corporations as well. Fortunately, Access Smart, creator of Power LogOn, has a tool that can help.

This book shows you how Power LogOn software can protect you from this fast-growing crime and — in case all else fails and your information *is* compromised — offers some pointers for getting you back on your feet.

How This Book Is Organized

Online Identity Theft Protection For Dummies, Power LogOn Edition, is divided into two parts.

Part I: Understanding Identity Theft and Getting Protection

In this part, you get acquainted with what exactly is the difference between identity theft and identity fraud, who the targeted victims are, and the tools that identity thieves use.

Chapter 1 discusses how we all use passwords as the gateway to our personal identities and company information, the need for strong password security, and why criminals seek out an individual's passwords. Chapter 1 also provides a brief summary of how Power LogOn can help increase security so that you are less likely to fall victim to identity crimes. Chapter 2 describes the threats and costs to companies that are targets of identity theft. Chapter 3 discusses the risks and costs to individuals as victims of identity fraud.

Part II: You Don't Have to be a Victim of Identity Crimes

This part clues you in on the proactive actions you can take to reduce your risks and covers what to do if you are the victim of an identity crime.

Chapter 4 shows you how to prevent becoming a victim by protecting yourself against physical and online theft. If you're responsible for a corporation or work in an IT department, you too get some pertinent information in this chapter. Chapter 5 helps you get started on the long path to recovering from an identity crime. This chapter is just a starting point. If you fall victim, pick up a more complete reference, such as *Preventing Identity Theft For Dummies* by Mike Arata (Wiley). Chapter 6 lists a few basic tools to further reduce a company's or individual's risks of becoming a victim of identity theft or fraud.

Icons Used in This Book

No *For Dummies* book would ever be complete without icons, those little images on the left side of the page. These icons draw your eye to certain points that are of particular importance and worth emphasizing. Here's how they help.

Take these tidbits to heart, and you'll be well on your way to preventing identity theft.

Watch out for these pitfalls, or you'll be one step closer to calling your favorite credit bureau "not for fun."

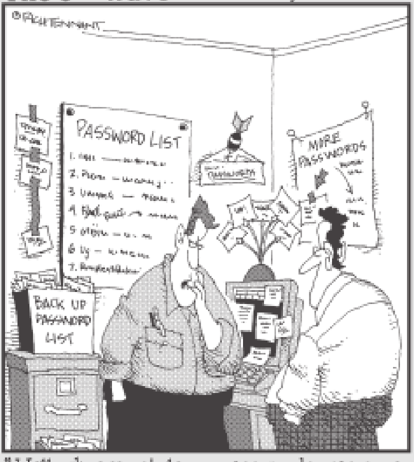
Pay special attention to these paragraphs, which can help you to make it or break it in your fight against crime.

This icon generally points out the, uh, technical aspects of creating safe password configurations.

Part I

Understanding Identity Theft and Getting Protection

The 5th Wave By Rich Tennant



"Well, whoever stole my passwords was sure clever. Especially since none of my reminders are missing."

In this part . . .

Online identity theft is the fastest growing crime in America. To protect yourself and your company, you need to understand how your computer password behaviors weaken the security of your identity online, what identity theft is, and what the costs are for not implementing proper security procedures. This part also shows you the benefits of using a new product called *Power LogOn*, which can help you to avoid becoming a victim.

Chapter 1

Talking about Password Security

In This Chapter

- Realizing that criminals crave your passwords
- Knowing that passwords are secure
- Understanding the problems with passwords
- Leveraging Power LogOn

For you or someone else to gain access to your personal accounts or company information, all that's needed is a legitimate password. So how secure is that password to your online bank account or human resources database? Here's a way to test it.

Do you, or maybe some coworkers you know, implement one or more of the following password management practices?

- Use a simple password based on a name, word, or date that can easily be remembered.
- Use a password that is very identifiable to that person, such as a kid's name with birth date, home town with zip code, and so on.
- Try to be clever and spell a child's name backwards.
- Use the same password everywhere and for everything.
- Write the passwords somewhere that others know to be a place where they're kept, such as in or on a notebook, piece of paper, white board, sticky notes, PDA, or whatever else happens to be handy.

- Have a Word or Excel document or some other data file called "passwords" that's stored in a computer.
- Have kids, spouses, and friends who know the passwords.
- Give office assistants account passwords.
- Keep the same password for years.
- Use the Web site's name as a password.
- Use the word *password* as a password.

If you answer "yes" to any one of these common password management practices, you are at risk of being a victim of online identity theft.

The preceding examples are just some of the more common password mistakes users make, and most users make a combination of mistakes.

Hackers break into computers and networks by breaking weak passwords, sending *phishing* emails (the practice of luring unsuspecting Internet users to a fake Web site where victims give out their passwords), creating fraudulent Web sites that request a password, downloading malicious programs onto your computer to snoop for passwords — and on and on goes the attack list. The reason that so many of these attacks are successful is because most people don't understand the attacks, don't know how to protect their computer, don't believe "it" will ever happen to them, and don't understand the importance of computer security even in the home.

Password *assignment* (the actual password) and *management* (the method used to remember a password) mistakes are common because remembering and typing complex passwords is cumbersome, coupled with the fact that too many of today's modern conveniences all require a password. So, you end up doing what's necessary to make computer security convenient — which makes it easier for you to get your work done.

The *worst* habit is writing your passwords on sticky notes and placing them on your computer monitor — bad, very bad. However, these very habits are what make some security consultants and developers of expensive cryptographic technologies claim that password security is insecure.

Why people practice poor password management

When people are asked why they use the same password everywhere, hide notes by their computer with their passwords on them, or create passwords that are too easy to remember, the answers almost always come down to one item: convenience.

- Most people cannot remember long, complex passwords.
- Most people have far too many networks, applications, and Web accounts that require a password.
- Most people have too much work to do and don't want computer security to be a barrier to meeting their deadlines.
- Companies and Web sites may require frequent password changes so the employee never has time to really memorize them.

Passwords are very secure; how people assign and manage their passwords is what causes the insecurity. Sadly, the weakest link is the individuals themselves. If security is seen as cumbersome, then human nature is such as to sacrifice one's own security for convenience. Online identity-theft criminals know and count on this human behavior to break in to computer systems easily.

Criminals Want Your Password

Passwords are used in more than 90 percent of all online and network security practices. People have passwords for online shopping, online banking, online stock trading, online travel planning, network logon, email accounts, voice mail, ATM, and so forth. On average, most people today have 20 or more different accounts that require passwords.

Companies use passwords to protect the personal information of their customers, employees, and vendors. Passwords are used to log on to the corporate network, where one has access to financial data, sales data, new product development, and a host of other confidential information. With all this information and money to be had through a simple password, no wonder the criminal wants it.

Information technology (IT) departments struggle with the task of either allowing employees to create their own passwords or assigning complex passwords to employees. Employees typically assign weak passwords, but complex IT-generated passwords result in IT spending more of their time resetting forgotten employee passwords. To avoid the embarrassment or hassle of contacting IT, employees will write their passwords on something and store them by their computers — which completely contradicts the reasons for having secure passwords. IT is in an ongoing battle with employees over their password security and their password convenience.

Creating Strong Passwords

A common theme throughout this book is that passwords are a secure way to identify yourself and protect data. The weakness frequently is in your creation and management of those passwords. So how do you create a strong password?

The way to determine the strength of a password is by its complexity, which is defined by its *length* (the number of characters), *character types* (numbers, upper case, lower case, and symbols), and *randomness* (the sequence of those characters). The purpose of a strong password is to force the thief or hacker to use password-breaking techniques that are less efficient. By meeting all these strength parameters, you force the thief into what is called a *brute force attack* — having to try every possible combination of these features until they find the right one. This attack is time-consuming and often detectable if being performed remotely onto a Web site or corporate network. Most thieves don't like this method because it tips off the IT security officer to start tracing the thief's location, which can lead to a thief's arrest.

To illustrate the strength of a complex password, a password made up of only four numbers (0 – 9) will take a *personal computer* (a PC) approximately 0.01 seconds to generate all possible combinations. When using a password created by selecting 20 out of 96 available characters, that same PC takes more than 40 gazillion years (picture 40 followed by 28 zeroes) to generate all possible combinations. Now you understand why IT security officers require complex passwords.

Passwords are just one way to authenticate yourself in the computer-security world. As users, you actually have three ways or *factors* to authenticate yourselves: *something I have, something I know*, and *something I am.*

- **Something I have:** Some physical item you possess, such as a key or smartcard
- **Something I know:** A password, PIN, or pass phrase you know
- **Something I am:** A physical characteristic that is unique to you, such as your fingerprint

The more that you combine these identification factors together, the stronger the security.

When you use only passwords — *something I know* — for identification, you have a single-factor authentication. When you store passwords on a smartcard — *something I have,* you then move up to a two-factor authentication. Finally, when a fingerprint scan — *something I am* — is required to authenticate yourself to the smartcard that stores your passwords, then you have the ultimate security of a three-factor authentication.

Managing Strong Passwords

Once you create a strong password, your next hurdle is how you remember it and how easy it is to type. Earlier I asked whether you know anyone who writes their passwords on notes by the computer, stores them in a document on their computer, or uses the same password everywhere. You probably do know someone like that, and it may even be you. I can approach almost anyone's computer and within minutes find their passwords. Being able to remember one complex 20-character-long password — let alone a hundred different ones —is by no means a reasonable expectation. Of course you have to write them down — or do you?

Now you have a way in which you never have to remember or type a password again.