SYNGRESS®

FREE E-BOOK DOWNLOAD

No Tech Hacking

A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing

- I've always had to keep super-cool secrets to myself. The head of the underground said so. But now, I'm airing all the underground's dirty laundry.
- Every book purchased can feed one African child for an entire month through a partnership with Action For Empowerment (AOET.org). See inside for more details.

HACKERS FOR CHARITY.ORG

Johnny Long

Scott Pinzon, CISSP, Technical Editor
Kevin D. Mitnick, Foreword Contributor

Visit us at

www.syngress.com

Syngress is committed to publishing high-quality books for IT Professionals and delivering those books in media and formats that fit the demands of our customers. We are also committed to extending the utility of the book you purchase via additional materials available from our Web site.

SOLUTIONS WEB SITE
To register your book, visit www.syngress.com/solutions. Once registered, you can access our solutions@syngress.com Web pages. There you may find an assortment of valueadded features such as free e-books related to the topic of this book, URLs of related Web sites, FAQs from the book, corrections, and any updates from the author(s).

ULTIMATE CDs
Our Ultimate CD product line offers our readers budget-conscious compilations of some of our best-selling backlist titles in Adobe PDF form. These CDs are the perfect way to extend your reference library on key topics pertaining to your area of expertise, including Cisco Engineering, Microsoft Windows System Administration, CyberCrime Investigation, Open Source Security, and Firewall Configuration, to name a few.

DOWNLOADABLE E-BOOKS
For readers who can't wait for hard copy, we offer most of our titles in downloadable Adobe PDF form. These e-books are often available weeks before hard copies, and are priced affordably.

SYNGRESS OUTLET
Our outlet store at syngress.com features overstocked, out-of-print, or slightly hurt books at significant savings.

SITE LICENSING
Syngress has a well-established program for site licensing our e-books onto servers in corporations, educational institutions, and large organizations. Contact us at sales@syngress.com for more information.

CUSTOM PUBLISHING
Many organizations welcome the ability to combine parts of multiple Syngress books, as well as their own content, into a single volume for their own internal use. Contact us at sales@syngress.com for more information.

SYNGRESS®

KEY	SERIAL NUMBER
001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	BAL923457U
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY
Syngress Publishing, Inc.
Elsevier, Inc.
30 Corporate Drive
Burlington, MA 01803

Printed in the United States of America
1 2 3 4 5 6 7 8 9 0

ISBN 13: 978-1-59749-215-7

Publisher: Andrew Williams
Technical Editor: Scott Pinzon
Page Layout and Art: SPi

For information on rights, translations, and bulk sales, contact Matt Pedersen, Commercial Sales Director and Rights, at Syngress Publishing; email m.pedersen@elsevier.com.

Johnny Long, Author

What's the story with the proceeds?

It's simple, really. My proceeds from this book are going to AOET (aoet.org), an organization that provides food, education and medical care to children left in the wake of Africa's HIV/AIDS epidemic. More than an aid organization, AOET aims to disrupt the cycle of poverty and hopelessness in sub-Saharan Africa through empowerment programs and job training, enabling children and adults to be self-sustaining, restoring not only their health but their pride and hope for a brighter future. A single book purchase made through my Amazon associates account (linked from any of my websites, or though http://tiniuri.com/f/Xpc) will generate enough income for AOET to feed a child for an entire month. Other retail purchases (which generate half as much income) will provide either medical services or educational supplies and funding for a single child through a donation pool set aside for those purposes. Because I am called to "look after orphans and widows in their distress" (James 1:27), and I know from personal experience how mutually transformative it can be to take that calling seriously. Hamlet was onto something when he wondered, "Whether this nobler in the mind to suffer the slings and arrows of outrageous fortune or to take arms against a sea of troubles, and by opposing, end them."

"I'm Johnny. I Hack Stuff."

There are many people to thank this time around, and I won't get to them all. But I'll give it my best shot. First and foremost, thanks to God for the many blessings in my life. Christ for the Living example, and the Spirit of God that encourages me to live each day with real purpose. This book is more a "God thing" than a "Johnny thing." Thanks to my wife and four wonderful kids. Words can't express how much you mean to me. Thanks for putting up with the real me.

I'd like to thank the members of the Shmoo group for fielding lots of questions, and to my book team: Alex, CP, Deviant, Eric, Freshman, Garland, Jack, Joshua, Marc, Ross, Russ, Vince and Yoshi. It was great to have your support, especially in such a tight timeframe. Thanks also to Scott Pinzon, for being a mentor and a great editor.

You've taught me so much. I'd also like to thank Vince Ritts for taking the time to plant no-tech hacking seed all those years ago.

And to the many friends and fans that have supported my work over the years, a final thanks. You make it very difficult to remain anti-social.

Be sure to check out our companion website at http://notechhacking.com as we continue the story of the no-tech hacker.

Johnny Long is a Christian by grace, a professional hacker by trade, a pirate by blood, a ninja in training, a security researcher and author. He can be found lurking at his website (http://johnny.ihackstuff.com). He is the founder of Hackers For Charity (http://ihackcharities.org), an organization that provides hackers with job experience while leveraging their skills for charities that need those skills.

Technical Editor

Scott Pinzon, CISSP, is Editor-in-Chief for LiveSecurity, a service offered by WatchGuard Technologies in Seattle. Pinzon has edited, written, and/or published well over 1,500 security alerts and "best practices" articles to LiveSecurity subscribers, who have tripled in number during his tenure. Pinzon has worked in the fields of security, encryption products, e-commerce, and voice messaging, with 18 years of experience writing about high-tech products for clients both large (Weyerhaeuser IT) and small (Seattle's first cash machine network). LiveSecurity training videos that Pinzon has co-written and directed have accumulated more than 100,000 views on Google Video and YouTube. He also hosts the internationally respected podcast, Radio Free Security. Pinzon was story editor for *Stealing the Network: How to Own a Shadow*, available from Syngress. He still believes he made the right call when he turned down the publisher who asked him to ghost-write books for Mr. T. AU1

Contributing Author

Jack Wiles is a security professional with over 30 years' experience in security-related fields, including computer security, disaster recovery, and physical security. He is a professional speaker and has trained federal agents, corporate attorneys, and internal auditors on a number of computer crime-related topics. He is a pioneer in presenting on a number of subjects that are now being labeled "Homeland Security" topics. Well over 10,000 people have attended one or more of his presentations since 1988. Jack is also a cofounder and president of TheTrainingCo. He is in frequent contact with members of many state and local law enforcement agencies as well as special agents with the U.S. Secret Service, FBI, U.S. Customs, Department of Justice, the Department of Defense, and numerous members of high-tech crime units. He was also appointed as the first president of the North Carolina InfraGard chapter, which is now one of the largest chapters in the country. He is also a founding member and "official" MC of the U.S. Secret Service South Carolina Electronic Crimes Task Force.

Jack is also a Vietnam veteran who served with the 101st Airborne Division in Vietnam in 1967–68. He recently retired from the U.S. Army Reserves as a lieutenant colonel and was assigned directly to the Pentagon for the final seven years of his career. In his spare time, he has been a senior contributing editor for several local, national, and international magazines.

Foreword Contributor

With more than fifteen years of experience in exploring computer security, **Kevin Mitnick** is a largely self-taught expert in exposing the vulnerabilities of complex operating systems and telecommunications devices. His hobby as an adolescent consisted of studying methods, tactics, and strategies used to circumvent computer security, and to learn more about how computer systems and telecommunication systems work.

In building this body of knowledge, Kevin gained unauthorized access to computer systems at some of the largest corporations on the planet and penetrated some of the most resilient computer systems ever developed. He has used both technical and non-technical means to obtain the source code to various operating systems and telecommunications devices to study their vulnerabilities and their inner workings.

As the world's most famous hacker, Kevin has been the subject of countless news and magazine articles published throughout the world. He has made guest appearances on numerous television and radio programs, offering expert commentary on issues related to information security. In addition to appearing on local network news programs, he has made appearances on 60 Minutes, The Learning Channel, Tech TV's Screen Savers, Court TV, Good Morning America, CNN's Burden of Proof, Street Sweep, and Talkback Live, National Public Radio, and as a guest star on ABC's new spy drama "Alias". Mitnick has served as a keynote speaker at numerous industry events, hosted a weekly talk radio show on KFI AM 640 in Los Angeles, testified before the United States Senate, written for Harvard Business Review and spoken for Harvard Law School. His first best-selling book, *The Art of Deception*, was published in October 2002 by Wiley and Sons Publishers. His second title, *The Art of Intrusion*, was released in February 2005.

Special Contributors

Alex Bayly approaches perfectly normal situations as though he were prepping a social engineering gig, much to the irritation of his wife. This habit has resulted in a rather large collection of pointless and frankly useless discarded ID cards for people he doesn't even know. He currently is employed as a senior security consultant in the UK, conducting social engineering work and traditional penetration testing.

CP is an active member of DC949, and co-organizer of Open CTF, the annual Open hacking contest at DefCon. Working officially as a software architect, his true passion lies in information security. He has developed several open source security tools, and continues his work on browser based security. Currently, CP is working on expanding oCTF, and opening human knowledge as a whole.

Matt Fiddler leads a Threat Management Team for a large Fortune 100 Company. Mr. Fiddler's research into lock bypass techniques has resulted in several public disclosures of critical lock design flaws. Mr. Fiddler began his career as an Intelligence Analyst with the United States Marine Corps. Since joining the commercial sector in 1992, he has spent the last 15 years enhancing his extensive expertise in the area of UNIX and Network Engineering, Security Consulting, and Intrusion Analysis.

When he's not dragging his knuckles as a defcon goon or living the rock-star lifestyle of a shmoo, **freshman** is the clue-by-4 and acting President of The Hacker Foundation. His involvement in the security/Information Assurance realm has been a long treacherous road filled with lions, tigers, and careless red teams. When he's not consulting, he can be found getting into heated discussions regarding operational security, Information Assurance best practice, and trusted computing over a bottle of good scotch.

Russell Handorf currently works for a prominent stock exchange as their senior security analyst and also serves on the board of directors for the FBI's

Philadelphia InfraGard Chapter. Prior to this, Mr. Handorf consulted for the US federal and state and local governments, law enforcement, companies and educational institutions where he performed training, security audits and assessments. His industry experience started as the CIO and director of research and development for a Philadelphia based wireless broadband solutions provider.

Ross Kinard is currently a senior a Lafayette High School. Ross works doing cleaning, god-awful cooking, and labor dog services. A constant interest in bad ideas and all types of physical security has kept him entertained with projects from pneumatic cannons to lockpicking.

Eric Michaud is currently a Computer and Physical Security Analyst for the Vulnerability Assessment Team at Argonne National Laboratory. A co-founder of The Open Organisation Of Lockpickers (TOOOL) - US Division and is actively involved in security research for hardware and computer security. When not attending and collaborating with fellow denizens at security events locally and international he may be found residing in the Mid-West. Though classically trained as an autodidact he received his B.S. from Ramapo College of New Jersey.

While paying the bills as a network engineer and security consultant, **Deviant Ollam**'s first and strongest love has always been teaching. A graduate of the New Jersey Institute of Technology's "Science, Technology, & Society" program, he is fascinated by the interplay between human values and developments in the technical world. A fanatical supporter of the philosophy that the best way to increase security is to publicly disclose vulnerabilities, Deviant has given lockpicking presentations at universities, conferences, and even the United States Military Academy at West Point.

Marc Weber Tobias, Esq. is an Investigative Attorney and physical security specialist in the United States. He has written five law enforcement textbooks dealing with criminal law, security, and communications. Marc was employed for several years by the Office of Attorney General, State of South Dakota, as the Chief of the Organized Crime Unit. Mr. Tobias has lectured throughout the world to law enforcement agencies and consulted

with clients and lock manufacturers in many countries. His law firm handles internal affairs investigations for certain government agencies, as well as civil investigations for private clients. Mr. Tobias is also employed by both private and public clients to analyze high security locks and security systems for bypass capability and has been involved in the design of security hardware to prevent bypass. Marc Tobias, through www.security.org, has issued many security alerts regarding product defects in security hardware. Mr. Tobias authored *Locks, Safes, and Security*, the primary reference for law enforcement agencies throughout the world, and the companion, LSS+, the multimedia edition.

Contents

Foreword . . . . . **xvii**

Introduction . . . . . **xix**

Chapter 1 Dumpster Diving **1**
Introduction to Dumpster Diving 2

Chapter 2 Tailgating **13**
Introduction to Tailgating 14
Dressing the Part 17
Real-World Tailgating Exercise 24

Chapter 3 Shoulder Surfing **27**
What is Shoulder Surfing? 28
Outside of the box 30
Great Locations for Should Surfing 33
Electronic Deduction 39
Killer Real-Life Surfing Sessions 47
Military Intelligence 47
Airliner Espionage 50
Robbing a Bank 53
Robbing Banks in Uganda, Africa 58

Chapter 4 Physical Security **61**
Introduction 62
Lock Bumping 62
Shimming Padlocks (*With Deviant Ollam*) 63
Master Lock Combo Lock Brute Forcing 67
Toilet Paper vs. Tubular Locks 72
Electric Flossers: A Low-Tech Classic 73
Laptop Locks Defeated by Beer (*With Matt Fiddler and Marc Weber Tobias*) . . . 75
TSA Locks (*With Marc Weber Tobias*) 78
Gun Trigger Locks vs. Drinking Straw (*With Marc Tobias and Matt Fiddler*) . . . 80
Entry Techniques: Loiding (*aka the Old Credit Card Trick*) 83
Entry Techniques: Motion Sensor Activation 87
Bypassing Passive Infrared (PIR) Motion Sensors 90
Camera Flaring 92
Real World: Airport Restricted Area Simplex Lock Bypass 96

Chapter 5 Social Engineering: Here's How I Broke Into Their Buildings 101
Introduction 102
How Easy Is It? 102
Human Nature, Human Weakness 105
Hello? Is this thing on? 106
The Mind of a Victim 108
"Social engineering would never work against our company!" 108
What Was I Able to Social Engineer Out of Mary? 110
The Final Sting 110
Why did this scam work? 111
Countering Social Engineering Attacks 112
Be Willing To Ask Questions 112
Security Awareness Training 113
Posters 113
Videos 115
Certificates 117

Chapter 6 Google Hacking Showcase 121
Introduction to the Introduction 122
Introduction 122
Geek Stuff 123
Utilities 123
Open Network Devices 128
Open Applications 137
Cameras 143
Telco Gear 153
Power 160
Sensitive Info 166
Police Reports 175
Social Security Numbers 179
Credit Card Information 185
Beyond Google 190
Summary 195

Chapter 7 P2P Hacking 197
Understanding P2P Hacking 198
Real World P2P Hacking: The Case of the Naughty Chiropractor 212

Chapter 8 People Watching 217
How to "People Watch" 218

Chapter 9 Kiosks 227
Understanding Kiosk Hacking 228
Real World: ATM Hacking 239
Chapter 10 Vehicle Surveillance 245
How Easy Is Vehicle Surveillance? 246
Chapter 11 Badge Surveillance 259
Where Are Your Badges? 260
Electronic Badge Authentication 264
Real World Badge Surveillance 266
Epiloque Top Ten Ways to Shut Down No-Tech Hackers 273
Go Undercover 274
Shred Everything 274
Get Decent Locks 275
Put that Badge Away 276
Check Your Surveillance Gear 276
Shut Down Shoulder Surfers 277
Block Tailgaters 277
Clean your Car 278
Watch your Back Online 279
Beware of Social Engineers 279
Index 281

Foreword

Annually, I attend a number of security conferences around the world. One speaker that I never miss is Johnny Long. Not only is Johnny one of the most entertaining speakers on the security circuit, his presentations are filled with interesting ideas that are corner stoned in what should be the first defense in security mitigation. Common sense.

Not only does Johnny challenge you not to ignore the obvious and to be more aware of your surroundings, his no tech hacking takes on a MacGyver approach to bypassing expensive security technology that sometimes are wholly relied upon to secure data and the premises.

Every day, corporations spend thousands of dollars on high-tech security defenses, but fail to give attention to the simple bypasses that no-tech hackers can leverage to their benefit. In this book Johnny presents eye-opening exploits that security professionals must take into consideration. In their haste to complete tasks and move along to the next topic, many security managers are overlooking simple flaws that render their high-dollar technologies, useless.

It is this complacency by security departments to ignore the simple threats; attackers are given the upper hand during a compromise. An intruder will always pursue the path of least resistance in an attack, while many businesses plan for the Mission Impossible scenario. Johnny will surprise you by bypassing a physical lock with a hand towel, tailgating behind a group of employees to enter a building, digging in the trash to uncover sensitive proprietary information, using Google and P2P networks to dig up sensitive information posted by internal employees and consumers alike, and then

showing you how all of these things pooled together may provide the open door for an attacker to exploit you.

The most overlooked factor in securing a business is the people factor. The most expensive technologies will provide you no benefit if an attacker can call up an employee and convince them to turn it off or alter its setting to create a window of opportunity. Social engineering is perhaps the hacker's favorite weapon of choice. Why waste time on an elaborate technical compromise, when you can make a few phone calls to gather seemingly innocuous information from unsuspecting people and leverage them into opening the door?

In my past life as a black-hat hacker, social engineering enabled me to get my foot in the door in record time—minutes. Afterwards, I would have to find and exploit technical flaws to achieve my objectives. The example of social engineering that Jack Wiles provided in this book may appear to be too good to be true. It isn't. And that's just a single pretext—the human imagination could think of many, many more. The question is, would you or your co-workers, employers, or mom and dad fall for it? The chapter on social engineering will offer insight on how no-tech hackers manipulate their victims into what is probably the most common method of attack for which no technological solution will safeguard your information.

Both consumers and businesses will find valuable information that creates awareness, within the pages of Johnny's *No-Tech Hacking*. This book clearly illustrates the often-ignored threats that IT managers should take into consideration when designing security plans to protect their business. Not only will business find the content of this book riveting, consumers will also garner knowledge on methods to protect themselves from identity theft, burglary, and hardening their defenses on home systems maintained by a computer. Much like his *Google Hacking*, Johnny has once again offered an entertaining but thought-provoking look into hacking techniques and the ingenuity being utilized by your adversaries.

—Kevin Mitnick

Introduction

What Is "No-Tech Hacking?"

When I got into this field, I knew I would have to stay ahead of the tech curve. I spent many sleepless nights worming through my home network trying to learn the ropes. My practice paid off. After years of hard work and dedicated study, I founded a small but elite pen testing team. I was good, my *foo* strong. Networks fell prostrate before me. My co-workers looked up to me, and I thought I was The Man. Then I met Vince.

In his mid-40s, hawk-eyed, and vaguely European looking, Vince blended in with the corporate crowd; he was most often seen in a black leather trench coat, a nice dress shirt, dark slacks, black wing tips and the occasional black fedora. He had a definite aura. Tales of his exploits were legendary. Some said he had been a fed, working deep-black projects for the government. Other insisted he was some kind of mercenary genius, selling his dark secrets to the highest bidder.

He was brilliant. He could do interesting and seemingly impossible things. He could pick locks, short-circuit electronic systems, and pluck information out of the air with fancy electronic gear. He once showed me a system he built called a "van Eck" something-or-other.[1] It could sniff the electromagnetic radiation coming from a CRT and reassemble it, allowing him to eavesdrop on someone's computer monitor from a quarter mile away. He taught me that a black-and-white TV could be used to monitor

[1] http://en.wikipedia.org/wiki/Van_Eck_phreaking

900MHz cellular phone conversations. I still remember hunching over a table in my basement going at the UHF tuner post of an old black-and-white TV with a pair of needle-nosed pliers. When I heard a cellular phone conversation coming through that old TV's speaker, I decided then and there I would learn everything I could from Vince.

I was incredibly intimidated before our first gig. Fortunately, we had different roles. I was to perform an internal assessment, which emulated an insider threat. If an employee went rogue, he could do unspeakable damage to a network. In order to properly emulate this, our clients provided us a workspace, a network jack, and the username and password of a legitimate, non-administrative user. I was tasked with leveraging those credentials to gain administrative control of critical network systems. If I gained access to confidential records stored within a corporate database, for example, my efforts were considered successful. I had a near-perfect record with internal assessments and was confident in my abilities.

Vince was to perform a physical assessment that emulated an external physical threat. The facility had top-notch physical security. They had poured a ton of money into expensive locks, sensors, and surveillance gear. I knew Vince would obliterate them all with his high-tech superpowers. The gig looked to be a real slam-dunk with him working the physical and me working the internal. We were the "dream team" of security geeks.

When Vince insisted I help him with the physical part of the assessment, I just about fell over. I imagined a James Bond movie, with Vince as "Q" and myself (of course) as James Bond in ninja assault gear. Vince would supply the gadgets, like the van Eck thingamabob and I would infiltrate the perimeter and spy on their surveillance monitors or something. I giggled to myself about the unnatural things we would do to the electronic keypad systems or the proximity locks. I imagined the looks on the guard's faces when we duct-taped them to their chairs after silently rappelling down from the ceiling of the surveillance room.

I couldn't wait to get started. I told Vince to hand over the alien gadgets we would use to pop the security. When he told me he hadn't brought any gadgets, I laughed and poked him. I never knew Vince was a kidder. When he told me he really didn't bring any gear, I briefly considered pushing him over, but I had heard he was a black belt in like six different martial arts, so I just politely asked him what the heck he was thinking. He said we were going to be creative. The mercenary genius, the storm center of all the swirling rumors, hadn't brought any gear. I asked him how creative a person could be when attacking a highly secured building without any gear. He just looked at me and gave me this goofy grin. I'll never forget that grin.

We spent the morning checking out the site. It consisted of several multistory buildings and a few employee parking lots, all enclosed by protective fencing. Everyone came and went through a front gate. Fortunately, the gate was open and unguarded. With Vince driving, we rounded one building and parked behind it, in view of the loading docks.

"There," he said.

"Where?" I asked.

"There," he repeated.

Vince's sense of humor sucked sometimes. I could never quite tell when he was giving me crap. I followed the finger and saw a loading dock. Just past the bay doors, several workers carried packages around. "The loading dock?" I asked.

"That's your way in."

I made a "Pffft" sound.

"Exactly. Easy." he said.

"I didn't mean 'Pffft' as in *easy*. I meant 'Pffft' as in *there's people there* and you said *I* was going in."

"There are, and you are," he said. Vince was helpful that way. "Just look like you belong. Say hello to the employees. Be friendly. Comment on the weather."

I did, and I did. Then I did, and I did and I found myself inside. I walked around, picked up some blueprints of tanks and military-looking stuff, photocopied them and left. Just like that. I'm skipping the description of my heart pounding at 400 beats per minute and the thoughts of what military prison would be like and whether or not the rumors about Bubba were true, but I did it. And it was an incredible rush. It was social engineering at its simplest, and it worked wonders. No one questioned me. I suppose it was just too awkward for them. I couldn't hide my grin as I walked to the car. Vince was nowhere to be found. He emerged from the building a few minutes later, carrying a small stack of letter-sized paper.

"How did you get in?" I asked.

"Same way you did."

"So why didn't you just do it yourself?" I asked.

"I had to make sure it would work first."

I was Vince's guinea pig but it didn't really matter. I was thrilled and ready for more. The next building we targeted looked like an absolute fortress. There were no loading docks and the only visible entrance was the front door. It was wood and steel—too much like a castle door for my taste—and approximately six inches thick, sporting a proximity card-reader device. We watched as employees swiped a badge,

pulled open the doors and walked in. I suggested we tailgate. I was on a roll. Vince shook his head. He obviously had other plans. He walked towards the building and slowed as we approached the front door. Six feet from the door, he stopped. I walked a step past him and turned around, my back to the door.

"Nice weather," he said, looking past me at the door.

"Ehrmm, yeah," I managed.

"Good day for rock climbing."

I began to turn around to look at the building. I hadn't considered climbing it.

"No," he said. "Don't turn around. Let's chat."

"Chat?" I asked. "About what?"

"You see that Bears game last night?" he asked. I had no clue what he was talking about or even who the Bears were but he continued. "Man, that was something else. The way that team works together, it's almost as if…" Vince stopped in mid-sentence as the front door opened. An employee pushed the door open, and headed towards the parking lot. "They move as a single unit," he continued. I couldn't help myself. I turned around. The door had already closed.

"Crap," I said. "We could have made it inside."

"Yes, a coat hanger."

Vince said strange stuff sometimes. That was just part of the package. It wasn't crazy-person stuff, it was just stuff that most people were too dense to understand. I had a pretty good idea I had just witnessed his first crazy-person moment. "Let's go," he said. "I need a washcloth. I need to go back to the hotel." I had no idea why he needed a washcloth, but I was relieved to hear he was still a safe crazy person. I had heard of axe murderers, but never washcloth murderers.

We passed the ride back to the hotel in silence; Vince seemed lost in his thoughts. He pulled up in front of the hotel, parked, and told me to wait for him. He emerged a few minutes later with a wire coat hanger and a damp washcloth. He tossed them into the back seat. "This should work," he said, sliding into his seat and closing the doors. I was afraid to ask. Pulling away from the hotel, he continued. "I should be able to get in with these."

I gave him a look. I can't exactly say what the look was, but I imagine it was somewhere between "I've had an unpleasant olfactory encounter" and "There's a tarantula on your head." Either way, I was pretty convinced he'd lost his mind or had it stolen by aliens. I pretended not to hear him. He continued anyhow.

"Every building has to have exits," he said. "Federal law dictates that in the case of an emergency, exit doors must operate from the inside out without the user having

any prior knowledge of its operation." I blinked and looked up at the sky through the windshield. I wondered if the aliens were coming for me next. "Furthermore, the exit must not require the use of any key or special token. Exit doors are therefore very easy to get out of."

"This has something to do with that door we were looking at, doesn't it?" I asked. The words surprised me. Vince and I were close to the same operating frequency.

He looked at me, and then I knew what *my look* looked like. I instinctively swatted at the tarantula that I could practically feel on my head. "This has *everything* to do with that door," he said, looking out the front window and hanging a left. We were headed back to the site. "The front door of that facility," he continued, "is formidable. It uses a very heavy-duty magnetic bolting system. My guess is that it would resist the impact of a 40-mile-an-hour vehicle. The doors are very thick, probably shielded, and the prox system is expensive."

"But you have a washcloth," I said. I couldn't resist.

"Exactly. Did you notice the exit mechanism on the door?"

I hadn't, and bluffing was out of the question. "No," I admitted.

"You need to notice *everything*," he said, pausing to glare at me. I nodded and he continued. "The exit mechanism is a silver-colored metal bar about waist-high."

I took my shot. "Oh, right. A push bar." The term sounded technical enough.

"No, not a push bar." Access denied. "The bar on that door is touch-sensitive. It doesn't operate by pressure; it operates when it senses it has been touched. Very handy in a fire." We pulled through the site's gate and parked. Vince unbuckled and grabbed the hanger and the washcloth from the back seat. He had untwisted the hanger, creating one long straight piece of strong, thin wire. He folded it in half, laid the washcloth on one end and folded the end of the hanger around it, then bent the whole thing to form a funny 90-degree-angled white washcloth flag. I smartly avoided any comment about using it to surrender to the guards. "Let's go," he said.

We walked to the front door. It was nearly 6:00 P.M. and very few employees were around. He walked up to the door, jammed the washcloth end of the hangar between the doors at waist height and started twisting the hanger around. I could hear the washcloth flopping around on the other side of the door. Within seconds, I heard a muffled *cla-chunk* and Vince pulled the door open and walked inside. I stood there gawking at the door as it closed behind him. The door reopened, and Vince stuck his head out. "You coming?"

The customer brief was a thing to behold. After the millions of dollars they had spent to secure that building, they learned that the entire system had been defeated with a washcloth and a wire coat hanger, all for want of a $50 gap plate for the door. The executives were incredulous and demanded proof, which Vince provided in the form of a field trip. I never learned what happened as a result of that demonstration, but I will never forget the lesson I learned: the simplest solutions are often the most practical.

Sure we could have messed with the prox system, figured out the magnetic tolerances on the lock or scaled the walls and used our welding torches—just like in the movies—to cut a hole in the ceiling, but we didn't have to. This is the essence of no-tech hacking. It requires technical knowledge to reap the full benefit of a no-tech attack, but technical knowledge is not required to repeat it. Worst of all, despite the simplicity, a no-tech attack is perhaps the most deadly and misunderstood.

Through the years, I've learned to follow Vince's advice. I now notice *everything* and I try to keep complicated thinking reigned in. Now, I'm hardly ever off duty. I constantly see new attack vectors, the most dangerous of which can be executed by anyone possessing the will to do so.

The Key to No-Tech Hacking

The key to no-tech hacking is to think simply, be aware, and to travel eyes open, head up. For example, when I go to a mall or some other socially dense atmosphere, I watch people. To me, strangers are an interesting puzzle and I reflexively try to figure out as much about them as I can. When I pass a businessman in an airport, my mind goes into overdrive as I try to sense his seat number and social status; make out his medical problems; fathom his family situation (or sense his sexual orientation); figure out his financial standing; infer his income level; deduce his dietary habits; and have a guess at his home address. When I go to a restaurant, I drift in and out of conversations around me, siphoning interesting tidbits of information. My attention wanders as I analyze my surroundings, taking it all in. When I walk through the parking lot of a building, I check out the vehicles along the way to determine what goes on inside and who the building's residents might be. I do all this stuff not because of my undiagnosed attention deficit disorder but because it's become a habit as a result of my job. I have personally witnessed the power of perception. When faced with tough security challenges, I don't charge. I hang back and I watch. A good dose of heightened perception levels the playing field every time.

—Johnny Long

Chapter 3

Shoulder Surfing

Dude. Surfing on your shoulder? Whoa. No, it's not a surfing-gymnastics mash up, but it is a sport—a hacker sport. Forget what you think you know about hackers eyeballing your password as you poke it out on your keyboard. We're talking about the X-Games version where hackers suck super-secret data of a laptop using only their minds. No psychic friends network here, just pure caffeinated hacker ingenuity. If you like having a screen on your laptop so you can see what you're working on, don't read this chapter. Because you might just want to rip your laptop's screen clean off when you experience shoulder surfing through the eyes of a no-tech hacker.

What is Shoulder Surfing?

Shoulder surfing is a classic no-tech attack that's been around about as long as shoulders themselves. It's a simple attack. All a bad guy does is peer over a victim's shoulder to see what he or she is up to. Back in the old days (before 1990 or so) this technique was used to snag calling card digits as a victim entered them into a public pay phone. A thief could reuse those digits to make free long distance calls, or sell them to others for less than market value. Although there are much easier ways to capture calling card digits these days, the skill of keypad monitoring still has many very practical uses. For example, consider the security screen below, presented at the cash register of an office supply store.

Like all the terminals located throughout the store (including many customer accessible terminals), this one prompts for an employee number and password. The kiosk allows access privileges based on the credentials entered. A manager will obviously have a higher level of access than an employee or a customer (who typically has no credentials). For certain transactions, such as the return of a high-value item, a manager login is required. As the next photo shows, a skilled keypad watcher (or cell phone video cam user) can capture the keystrokes as they are entered.

A no-tech hacker could then reuse those credentials at a customer terminal to do all sorts of interesting (read: nasty) things.

Keep Those Digits to Yourself

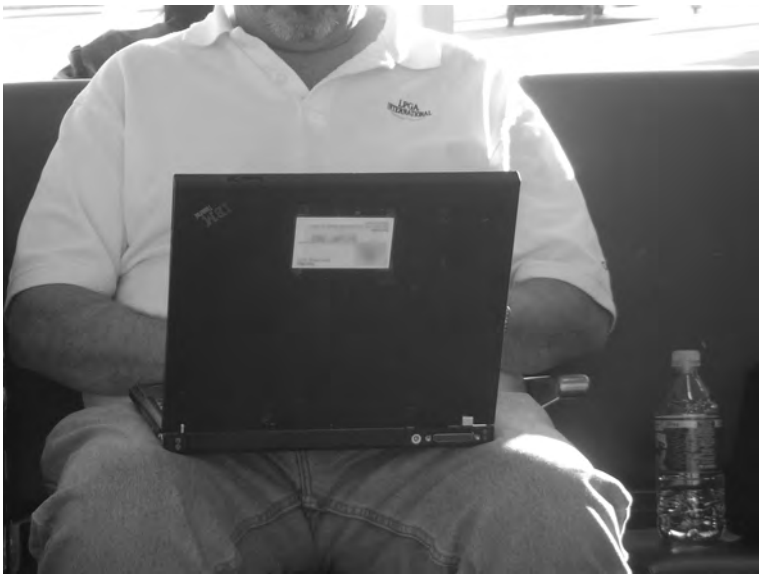
What's the point of requiring a pass code if you enter it in plain site of everyone? When entering sensitive data, create some sort of barrier between the keys and wandering eyes. This might require you to reposition your body, or create a shield with your spare hand. If you aren't willing to do this, why have a pass code at all?

Keypad data capture is still pretty old school, though. When the world went digital, shoulder surfers turned their glances from keypads to keyboards, hunting not for calling card numbers, but for passwords. This is no easy trick. Every time I try to pull it off, I'm reminded of the classic move *Sneakers*. The entire hacker "dream team" was

baffled by video footage of a mathematician entering his password. Rewinding the footage, they eventually realized the password was indiscernible—the victim was just in the way. Fortunately, this chapter isn't about catching those fleeting passwords. It's about being observant and realizing that shoulder surfers have evolved beyond keyboard-watching.

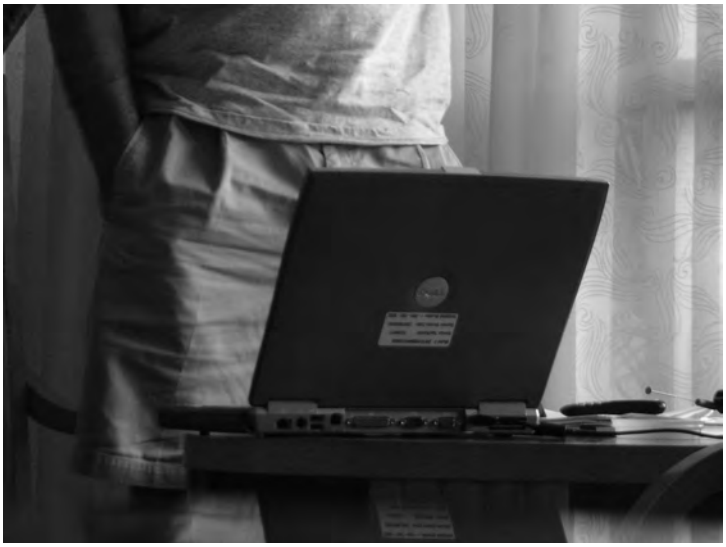
Outside of the box

Before we get into actual shoulder surfing technique, let's first talk about how easy it is to profile a target by looking at the machine itself. Consider the traveler shown in the next photo.



A true techie would probably already have figured out the age and model of the IBM ThinkPad based solely on the design of the machine and the ports on the back. A hacker might swing around behind the machine to get a glimpse of the screen in an attempt to learn more about this target. But a decent no-tech hacker (or an astute observer) would instead check out the business card taped to the laptop lid which reveals the target's name, company, job title, address, office phone and cell phone number. The tape-on business card phenomenon is becoming quite the rage. I see them everywhere these days. Here's another one I captured in the wild.

A relative of the tape-on business card is the company-supplied inventory sticker. Many times these are simple tiny barcode stickers, but some (like the one shown in the next photo) are larger, and reveal quite a bit of information.



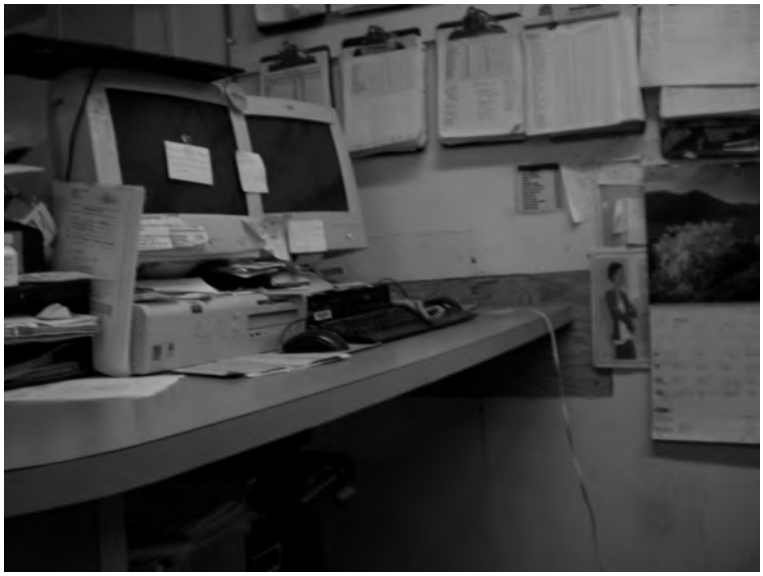
Check out the undisputed king of corporate stick-on I captured in the next photo.

Not only does this poor laptop sport a corporate inventory sticker, it's adorned with a corporate logo and a super-bright hot orange sign that screams "ultra sensitive" in English and what I guess is Chinese. Even an illiterate laptop thief might get the clue that this laptop is one worth stealing. This brings up an important point. While laptop stickers can be used to profile a victim, they can also serve to mark a laptop as valuable, making the owner a target for theft or physical violence. I'm reminded of the U.S. Government "Classified," "Secret," and "Top Secret" stickers which I've seen in the field. While I understand the practical value of these stickers in a mixed-classification government environment, I've seen way too many of them out in the wild. Even the benign "Unclassified" sticker is an indication that the device is used in or around government spaces, making the device a target for thieves, spies and UFO conspiracy theorists.

Say "No" to Stickers

Those stickers have got to go. If you're forced to have them on your gear, consider putting a sticky note over them when you're traveling. This will at least keep the sticker (and the information that can be inferred from it) hidden from too-curious eyes.

It's impossible to have a no-tech discussion about stickers without mentioning the most famous sticky of them all: the Post-It note. I can't tell you how many sticky notes I've seen in my travels. They often appear on monitors and desks and almost always contain interesting information a no-tech hacker can take advantage of. I discovered the machines below sitting unattended inside a fancy hotel's loading dock.



Pay no mind to the paperwork that fills every nook and cranny and nearly every square inch of wall space. Try to focus beyond the unlocked file cabinets and instead have a look at the computer systems and those gorgeous sticky notes. Most are useless to my eyes, but one contained what looked like login credentials, which (judging from the network cable) authenticate to the hotel network—the same network that serves the guest registration database. A no-tech hacker can gather plenty of information without touching a single machine or committing a single crime. And if someone catches him in the room? Well, he's just a confused guest in search of a bathroom. Good luck proving otherwise.

Great Locations for Should Surfing

There are many great locations for shoulder surfing, but some are better than others. First, let's talk about airports.

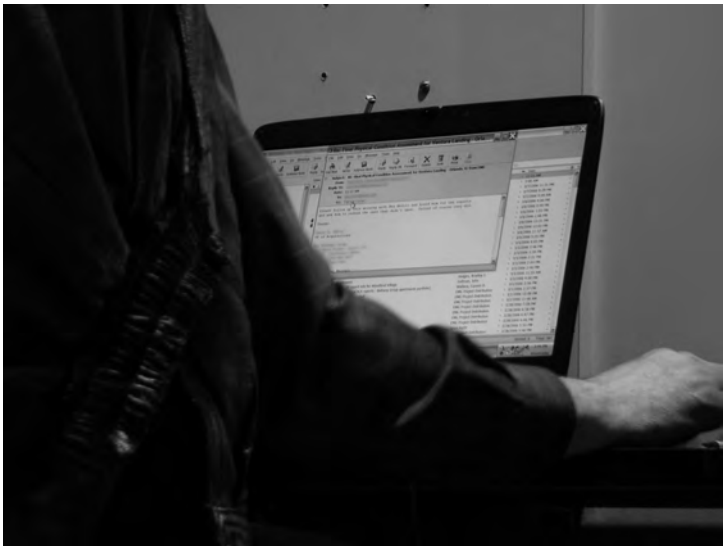
The first shoulder-surfing opportunity at an airport occurs during check-in, especially at the self-service kiosks, which we talk more about in Chapter 9. Check-in kiosks clearly display information such as the traveler's name, destination, seating assignment

and frequent flier number during the check-in process. Security checkpoints also offer the unique (and unsettling) opportunity to shoulder-surf TSA agents as they go about their business.

Since hanging around security checkpoints taking photos of TSA agents isn't such a smart idea, a no-tech hacker will inevitably head for the executive lounge, where he'll either legitimately enter or social engineer his way inside. These lounges are often packed with high-profile people doing high-profile things, most of whom are oblivious to shoulder surfers.

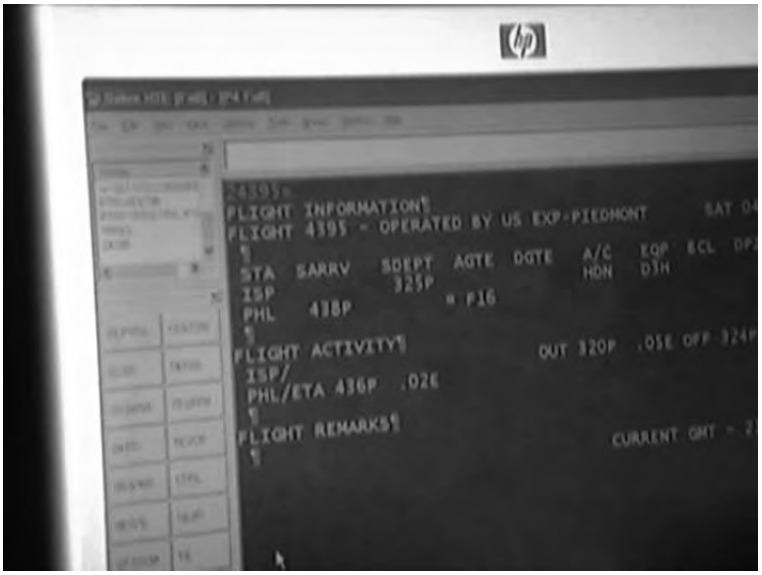
There's great fun to be had at the gates as well, thanks to the back-to-back seating arrangement and the bustle and distraction made by a constant stream of weary travelers. The photo below was taken in this sort of environment.

Despite the awkward angle and horrible lighting, the screen is still perfectly readable (I have blurred the screen to protect the user's crystal-clear Outlook email session). Semi-private kiosks provide even better lighting, making it much easier for a surfer that's quite a distance away. The Vice President of Acquisitions shown in the next photo was oblivious to my presence as he pecked out a confidential inter-department email.



Lounges in and around airports offer great surfing opportunities as well, as shown in the next photo.

Although airport systems are hardly ever a target for most no-tech hackers, it's impossible not to notice unattended airport personnel workstations. The airline Sabre system shown in the next photo is practically begging to be tinkered with.



Coffee shops are another favorite hangout for shoulder surfers, as shown in the next few photos.

It seems that the more comfortable the environment, the less wary it's patrons tend to be. I've personally seen everything from architectural designs (shown in the next photo) to confidential emails to government proposal documents being edited in coffee shops, and other no-tech hackers have told me tales of even more interesting things.

Business lounges offer great opportunities for kiosk hackers (discussed in Chapter 9) but also for shoulder surfers, as shown in the next photo.

If it's important enough to work on in a hotel business lounge, it's probably pretty important. Shoulder surfers know this. Keep aware.

Keep It Secret, Keep It Safe

Sorry for the blatantly geeky Lord of The Rings quote, but Gandalf's got it right. Keep your private stuff from public consumption. Don't work on your personal stuff in public spaces, and don't make yourself a target. Be aware of the profile you are presenting, and tone it down if necessary. If you've got to work on private stuff in public, consider a laptop privacy filter (try a Google search for "laptop privacy filter"). Of course bear in mind that an experienced shoulder surfer will see a privacy filter and rightly assume you're working on something sensitive. Because of this, the mere existence of a filter can make you or your machine a target. Did I mention leaving the private stuff out of public spaces? That's your best bet.

Electronic Deduction

Information is certainly more valuable than hardware, and professional thieves understand this. Although an amateur thief may have a decent understanding of the relative value of something like a laptop based on it age and hardware specifications, a professional will often use no-tech techniques to determine the relative value of the data stored on a machine by profiling the machine's user. We've already looked at a few interesting external clues, but the best way to profile a machine's owner is to get a look at the screen.

StankDawg (http://www.stankdawg.com) released a paper entitled *The Art of Electronic Deduction* (http://www.docdroppers.org/wiki/index.php?title=The_Art_of_Electronic_Deduction) which explored the methods an attacker can use to glean information from interesting electronic sources. Taking a cue from his paper, check out the photo below of a temporarily unattended laptop I spotted in a coffee shop.

I have altered the image to keep the owner's company name confidential, but by using the information on the screen, an accomplished no-tech hacker can glean an awful lot of information. For starters, the desktop background indicates that the laptop is running Windows XP Professional. Other aesthetic clues such as the Start button configuration back this up. The operating system of a machine is a necessary piece of information a technical attacker can use to determine the type of attack to launch. Generally, an attacker would need to analyze a series of network packet responses to

determine this information, but in this case that is unnecessary–it is unlikely the laptop's owner has installed another operating system's desktop background. Focusing on the icons on the desktop, we can immediately deduce the company the user works for as one icon (blurred in the above image) spells it out clearly. The icons below help us deduce even more.

The word *sales* indicates that this is some sort of sales software, but a Google search reveals that SalesLogix is the leader in mid-market CRM (customer relationship management) software. The search goes on to say that SalesLogix is "the most powerful sales tool on the Web." We can confidently deduce that the owner is in a sales position. The icons below refer to *SAP*, a common business software solution provider.

The existence of the SAP logon client indicates the logon credentials for the service may be installed on the laptop as well. If a thief were to make off with this machine, there's a decent chance he or she may be able to log into the company's SAP system using stored credentials. The icon below is titled *SecuRemote*.

A Google search reveals that *SecuRemote* is a virtual private network (VPN) client. As with the SAP logon software, all or part of the VPN credentials may reside on the laptop, allowing an adversary access to the corporate network. At the very least, the mere existence of a particular brand of VPN is valuable information to a technical attacker.

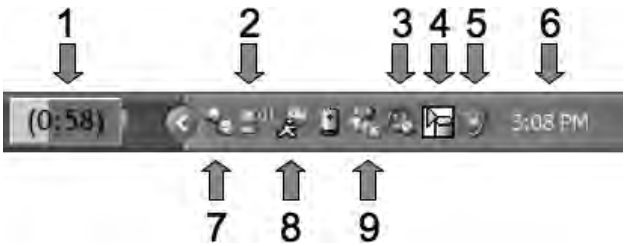
The icons below reveal that Palm personal digital assistant (PDA) software has been installed on the machine. The owner probably owns a Palm device, and the contents of that device are most likely backed up or synced to the laptop.

The icon below reveals the existence of the AT&T Global Network Client.

Again, this network client may have cached credentials, which might allow an adversary in possession of the laptop to log in as the machine's owner. An unfortunately named icon is shown below.

I can only hope that this document does not contain any sort of actual access code. That would make a bad guy's job *way* too easy.

Desktop icons provide a great deal of information, but a technically savvy attacker can learn even more by looking at other details on the screen. For example, what information can you determine by looking at the taskbar below?



This taskbar itself reveals an awful lot of information. The layout reveals that we're looking at a modern version of Windows, most likely Windows XP. But each of the icons has meaning as well. How many can you identify? Here's what each of the icons represents.

1. This is the battery indicator, which shows this machine is a laptop, and that there are fifty-eight minutes of battery power remaining. We can tell that the machine is not plugged into a power source because there is no electrical plug icon next to the battery.
2. This icon reveals that the machine is connected to (and communicating with) a wireless access point. The third icon.
3. This icon shows that the system speakers are muted.

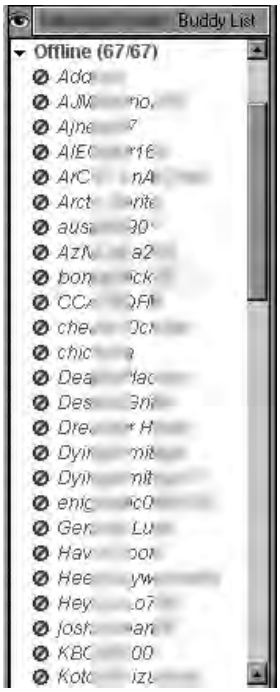
4. This is the IBM *Hard Drive Active Protection* program icon. It reveals that the machine is an IBM laptop, and that no system shocks have been detected (the machine has not been dropped recently).
5. This icon represents the Microsoft Security Center, which is currently disabled—meaning that the security level of the machine is less than optimal and may be vulnerable to attack. This is also verification that the machine is running a modern version of XP.
6. This is the system clock, which is set to 3:08 P.M. This information can be correlated with the current local time to help determine the time zone the owner originated in. If it's not set to where they are, it's set to where they're from.
7. This icon belongs to the Trillian instant messaging program. The Trillian website (www.ceruleanstudios.com) describes the program as "a fully featured, stand-alone, skinnable chat client that supports AIM, ICQ, MSN, Yahoo Messenger, and IRC." It goes on to say that "It provides capabilities not possible with original network clients, while supporting standard features…" In layman's terms, Trillian is an instant messaging client replacement. The style of the icon indicates that Trillian is connected and logged in.
8. This is the ever-popular AIM (AOL Instant Messaging) icon, and its style indicates that the program is connected to a server and that the user is logged in.
9. This icon belongs to Microsoft Instant Messenger (MSN), and its style reveals that the program is running, but the user is not logged on.
10. If it seems odd that this person is running Trillian, AIM, and MSN all at the same time, you've picked up on an interesting point. The Trillian software makes the AIM and MSN clients redundant. So beyond the fact that this person is probably looking for love in all the wrong places he or she is probably not all that technical—there seems to be little reason to be connected with both AIM and Trillian at the same time. The mere fact that these clients are in active use gives an observer grounds for more research since both MSN and AIM require users to sign up for an account online, and create a personal profile, which may contain personal information. Yahoo's instant messenger client is currently the most bloated in terms of add-ons and created online profiles. A Yahoo user has to be very careful not to reveal too much personal information.

Instant Messaging Profile Pitfalls

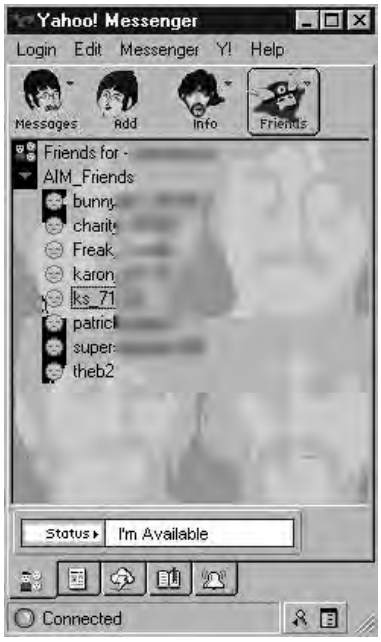
We could do an entire book on the privacy implications of using instant messenger programs. When signing up for an account, a new user creates all sorts of data trails that a hacker or identity thief could uncover. While we don't have the page space to go into all the potential pitfalls here, just understand that poorly configured IM clients are bad news if you're concerned about your privacy.

An online investigation of this IM user would at least require a username. If a chat window is left open, like the one provided by StankDawg below, the user's name is in plain site at the top of the window.

Armed with the logged-in user name, an observer could start an online information gathering exercise to profile the machine's owner. This exercise would include a search of the target's buddy's information as well. Armed with a well-populated buddy list (like the one shown below, also provided by StankDawg), an observer could delve deep into the personal life of a target, beginning with the least privacy-conscious buddy's profile first.



Sometimes the names on a buddy list aren't nearly as important as the appearance of the buddy list itself. StankDawg provides the Yahoo Instant Messenger buddy list show below.



It's obvious that this user is a Beatles fan. A social engineer could leverage this information as a conversation starter. As StankDawg says, an observer can create a "preponderance of evidence" which uses seemingly useless coincidental evidence to build a profile of a target. When these bits of evidence come from multiple sources—screen shots, body language, dress, mannerisms, etc—an observer can build an amazingly accurate profile of a potential target.

But any profile built this way can be flawed. The best no-tech hacker realizes this and does not discount a single piece of evidence. Consider the expanded taskbar shown below. It is an expanded version of the instant messenger junkie's taskbar we discussed above.

There are lots of interesting icons that weren't visible before, but the one marked with the arrow is particularly revealing. The onion icon represents Vidalia, a package that incorporates Tor (The Onion Router) and Privoxy, two tools used to anonymize a user's Internet activity. A user surfing the Web with Privoxy Tor enabled surfs in complete and utter anonymity. Remote Web sites can't tell where the user is coming from, and anyone sniffing the local network traffic can't see where the user is going. This tiny icon, consisting of no more than forty pixels, tells a great deal about the user of this machine. The user is no half-witted web surfer who doesn't know his AIM from his MSN. At the very least, he or she is a privacy advocate, and at the worst he or she is up to something nefarious. This speculation could be misguided, but the best of no-tech hackers can accurately distill all these interesting tidbits into fact and then make a decision based on those facts—all in a dizzyingly short period of time.

Gah! It's all too much! Help me!

The best defense is to remain aware when traveling. Don't put yourself in situations that invite shoulder surfers. Position your back to the wall when using your machine, and never leave your machine unattended. Don't wear company logos. Remove extraneous markings and information from your

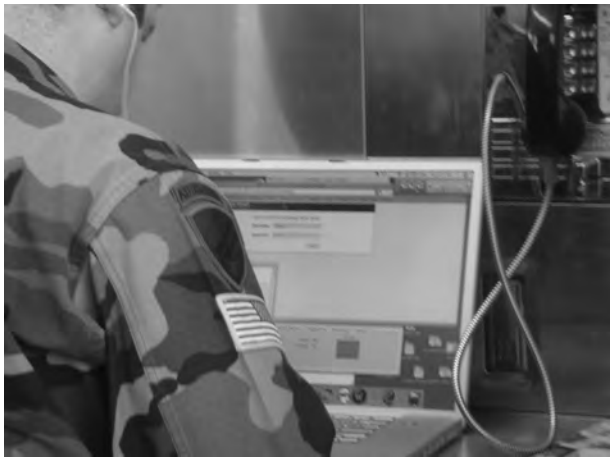
mobile computing devices, especially if your company name might entice an adversary. The tech support folks in your organization can probably provide you a long list of tech things to avoid when traveling. Follow their advice.

Electronic deduction is definitely an art. We could fill page after page with the topic but understand what we're getting at here—literally every square inch of your screen contains something of interest to a no-tech hacker. If you've got something on your machine that might tempt a thief or no-tech hacker, keep it out of the public eye. There's no sense making yourself a target.

Killer Real-Life Surfing Sessions

Military Intelligence

The best way to explain what goes on in the mind of a no-tech hacker is to show you. In this section, we'll take a look at some real-world shoulder surfing sessions. The first example centers on the guy in the next photo.



It's obvious that he's a member of the U.S. military. The insignia and patches on his uniform reveal quite a bit, especially to those with military knowledge. While certain adversaries might take an interest in him because of his military affiliation, any no-tech hacker can learn an awful lot by looking at the gear that surrounds this guy.

For starters it's obvious he's a Mac user. He's using a Mac PowerBook and his white headphones are an iPod signature item. The off-screen Mac Addict magazine seals the deal—he's a bona fide Apple fan-boy. Closer examination reveals that he's also a gamer.

The icons in his dock (shown below) mean that he's installed World of Warcraft (WoW) and Ventrillo voice communication software.

A social engineer might use this knowledge to his advantage, choosing to either engage him in a WoW or Windows-bashing conversation. But many no-tech hackers will avoid social engineering unless it's absolutely necessary. By moving in closer to surf this guy, an adversary can learn much, as we'll see.

But I have to say I am surprised to find this particular target with his back to the world and his headphones on, especially considering the "RoadWarrior" guide I discovered recently.

This guide includes a handy tear-off wallet card which reminds "road warriors" to "Ensure against public display of content: Shoulder Surfing." The guide also goes on to advocate being "a wary and alert traveler."

Still, as you can tell from the next photo, moving in on this guy is simple, thanks to his blaring headphones and his corner-facing position.

As it turns out, he's not casually surfing the Web—he's logging into the administrative console of a BEA WebLogic server. Given that Weblogic is heavyweight industrial-grade software, it's safe to assume that he's busy with work—perhaps even official

U.S. Government business. As he typed his credentials, I made a quick adjustment to my camera and took another photo. The flash fired, and the target turned around sharply, finally noticing me. I looked down at the camera and rubbed my eyes, pretending to be blinded by my own flash. He shrugged and returned to his work, convinced, I assume, that I was some kind of digital camera newbie just figuring out the ropes. This road warrior did not *want* to assume I was taking a picture of him. That, of course could create all sorts of unpleasantness for him. So he did what most portable computer users do–he assumed the best, and went back to his work. This makes the job of a no-tech hacker even easier.

Throw Down!

I'm not suggesting you body tackle every oddball that might be shoulder surfing you. What I would suggest is that you close your machine if you think you're a target and become interested in something else, like sipping your coffee. Most no-tech hackers will know they've been busted and move along. If they do, keep a casual eye on them as they leave and try to get a good look at them and their car/bike/skateboard/Segway before they bail. When they've cleared out take a look at what you were working on, consider all of it compromised, and act accordingly. If your surfer doesn't bail after you close your lid, keep an eye on him or her anyhow. If he or she continues acting suspiciously, do something about it. Inform a manager, security guard or hall monitor. Do *something*. If that something involves physical violence, just don't tell the judge it was my idea.

Airliner Espionage

Our next example takes place at 30,000 feet on board a commercial airliner. Airplanes are tough places to shoulder surf because a surfer is generally limited to checking out the people around him or in the aisles surrounding the rest rooms, where passengers tend to hang out. Hovering over a stranger's shoulder anywhere else gets the undercover air marshal all nervous.

Since I hardly ever get any sleep while traveling (who can sleep with all the no-tech hacking to do?) I was awake to catch the late-night laptop party happening in the next row.

At first, I wasn't all that interested since I was in the opposite window seat, and the aisle seat next to me was occupied by an awake and over-caffeinated stranger. Still, when my neighbor stood up to go to the bathroom, I couldn't resist the wide-open photo opportunity. I turned off my flash, and took the next photo.

The photo was boring and the angle was too sharp, but as I scoped the guy, I realized that his entire demeanor screamed *government*. His wing tips were nice, but not too nice. His binder was decidedly Government Issue, and the glance I stole of his laptop bag revealed what looked like a government insignia of some sort. I watched disinterested for a few more moments until my shot-blocking neighbor returned. As he settled into his seat, he grabbed the in-flight magazine and started flipping through it. Figuring my game of surf-the-fed was at an end; I closed my camera and tried to find something better to do. I remember feeling relieved. Despite how good the session might be, surfing is still hard work. But as fate would have it, the game wasn't quite over—it was just beginning. The fed pulled out a notebook stuffed with interesting-looking paperwork. Getting a shot of that paperwork from the other side of the plane seemed tricky, but I held up my jacket to form an impromptu curtain, flicked the zoom and took a quick shot. No one seemed to notice.

More paperwork surfaced and I felt drawn by it. Although I'm not usually the government employee stalker type, I just knew this guy was working on something significant, and he didn't seem to care who watched him do it. I accepted his invitation and eventually caught a glimpse of a juicy header page. I couldn't get my camera out fast enough to snap the next photo.

The page (written in monster header font) read *Government Systems EW/SIGINT 2006 Strategic Plan*. Any amateur GoogleDork can tell you that "EW/SIGINT" means Electronic Warfare Signals Intelligence in military-speak. I felt my pulse quicken as I realized I was at 30,000 feet surfing the government's 2006 strategic plan for their electronic warfare signals intelligence something-or-other. I immediately stopped taking photos of my careless Fed friend and have been stalked by black helicopters ever since. I'm not too freaked out by that though, because now I know how to disable their electronic systems with a cheap digital watch and a patch of duct tape. Although sometimes at night my wife complains about the noise.

Robbing a Bank

With their electronic and physical security systems, banks are in the Top Five list of high-security targets. But one thing I've come to learn in this business is that even the best security systems share a common flaw: lazy human beings. I really had no intention of robbing the bank in the next photo when I strolled by it.

But as I walked past the front door, I caught a glimpse of the bank manager sitting in his corner office working on his computer system. I stopped in my tracks and turned to look at him through the window. Although he was in my line of sight, he didn't seem to notice me. I pulled out my (ever present) camera, backed up a step and snapped the next photo.

Oblivious to my presence, he turned around and began working on some paperwork at his desk. Still standing in the same position, I zoomed my camera in and grabbed a photo of his screen. I reviewed the image and realized that the camera had focused on his blinds, making the on-screen text completely unreadable. The manager continued working at his desk, so I adjusted my focal length (which took me a while because it's something I rarely have to do) and snapped a few more photos. Eventually, I got a few like the one below, which captured the screen text in perfect clarity. (The area inside the box is unaltered—I have blurred the rest to protect the innocent.)

As I stood there reading the bank manager's screen on my camera's LCD screen, I had a realization–stealing money from a bank is *so lame*. The information housed by a bank is worth so much more than the actual liquid assets they have in the vault. Professional criminals and amateur identity thieves alike could easily liquidate a bank's information stores to reap millions of dollars in cold, hard (unmarked) cash, with far less risk than storming a lobby and taking hostages. I wondered how much one screen of personal information would fetch. As I pondered how rich I would be if I was one of the bad guys, the banker stood up from his desk and left his office unattended. I fiddled with the zoom again and snapped a few photos of the contents of his desk. Eventually the zoom settings cooperated and I captured a clear image of his paperwork.

I never imagined how simple it could be for a no-tech hacker to siphon information from a bank. I scoped the rest of his office and snapped some more photos like this next one.

I checked the images and found them all to be crystal-clear. After a few moments, the manager strolled back through his office door. As I stood there with my camera at eye level, aimed at his guest table, I wondered if I had liberated enough info to sell on the black market to pay my bail money. It hadn't dawned on me that he might actually have gone to alert security about his new voyeuristic hacker friend. He shuffled around the desk, adjusted his belt and his pants and plopped down into his overstuffed chair without casting me a single glance.

I waited a few stressful moments, fully expecting to be tasered by a trigger-happy bank rent-a-cop. It never happened. I turned and continued past the office, nearly bumping into an office employee out on a smoke break. The employee never noticed me—he was busy chatting on his cell phone, right outside the banker's office. I suddenly realized that the banker "tuned out" everyone lingering outside his office. He had gotten so used to passers by that now everyone outside his window (including no-tech hacker types with cameras) was a harmless irrelevance. Security guards often suffer from the same problem after watching a video monitor for hours on end. They get so used to nothing happening that when something finally does, they miss it.

Can I Get a Copy of Those Photos?

Uhmm, no. Let me say it again. I'm not one of the bad guys. If I were, I'd be either rich or in Cell Block 13 married to Bubba. As such, I've got a pretty high ethical standard and am only in the business of raising awareness about the threats I leverage in my professional life. I'm also not in the business of addressing every single potential threat I witness, like this bank problem. Most folks don't take too kindly to the likes of me poking at their stuff.

As I stood at the teller desk during a later (legitimate) visit to the bank, my eyes meandered to the tech gear behind the counter. I pulled out my camera phone and snapped the photo below.

The tiny, blurred, heavily altered (protecting my rear-end) photo of a printer isn't much to look at. Sorry. But I've included it for two reasons. First, it's possible to take a picture just about anywhere these days—even airport customs desks where the armed guards hang out and all the signs say "No Photographs."

The second reason I included the printer photo is not because of the printer itself, but because of the stickers on the top (blurred, etc, etc) which clearly list the name and telephone number of the I.T. company the bank uses for computer support. If you think that dressing up as the computer repairman only works in the movies, think again. I've done it successfully several times. And when I've done it I didn't have the luxury of knowing who the actual I.T. support company was.

Robbing Banks in Uganda, Africa

While on a recent mission trip to Uganda, Africa (see http://johnny.ihackstuff.com/uganda) I wasn't exactly in the no-tech hacker mindset. It was, after all, a wholly different place from my home in the United States. But as I stood at the ATM machine at one of the largest banks in Jinja, I couldn't help but notice that the bank had a strange sort of open iron fencing above each of the locked doors. Amused, I snapped the photo below.

As I looked at the photo in my viewfinder, my mind reeled with all the potential security problems this fencing presented. My mentor Vince would have had a field day with this type of setup. The coat hanger trick could probably be used to unlatch the door or block a security camera, or… My thoughts were interrupted by a nudge and I spun around. An unhappy-looking gentleman with a menacing looking rifle stood behind me. "No pictures. Put the camera away," he said, almost (but not quite) politely.

The rifle was impressive, and the uniform was even more impressive. His hat and lapel were emblazoned with a logo that read "Tight Security." The irony was thick. Here I was in a place that many would consider third-world, and I was facing perhaps the best security I had ever witnessed anywhere. I glanced over the man's shoulder and suddenly noticed that three other guards, similarly armed and dressed, were along the bank's outer perimeter.

"Friggin' sweet," I said with a smile.

The guard's expression sagged, his smile faded. "Put away the camera," he said.

I looked down and realized I still held the camera. I cleared my throat and put the camera away.

Friggin' sweet.

Epilogue

Top Ten Ways to Shut Down No-Tech Hackers

AU1

Now that we're clear on what the bad guys can accomplish, let's review what can be done to keep them at bay. Presented in no particular order, here are the ten best ways to shut down no-tech hackers. AU2

Go Undercover

Keep it Secret. Gandalf had it right when he said, "Keep it secret, keep it safe." Don't work on private stuff in public spaces, and don't make yourself a target. Be aware of the profile you present, and tone it down if necessary. If you've got to work on private stuff in public, consider a laptop privacy filter. Of course bear in mind that an experienced shoulder surfer will see a privacy filter and rightly assume you're working on something sensitive. Because of this, the mere existence of a filter can make you or your machine a target. Did I mention leaving the private stuff out of public spaces? That's your best bet.

Play it smart. You might be proud of the company you work for, but sometimes flying the team colors is a bad idea. Depending on current events, the political climate or other factors anyone can become a target of public scrutiny or unwanted attention. Government agencies have requested for years that employees travel low profile, but those same agencies still produce signature items sporting the agency logo. The best advice I can offer you is to play it smart. Take a moment to consider your profile, and every now and then play it paranoid. A no-tech hacker may be the least of your worries.

Say no to Stickers. If you're forced to have company stickers on your gear, consider putting a sticky note over them when you're traveling. This will at least keep the sticker (and the information that can be inferred from it) hidden from too-curious eyes.

Let's (not) Go To Lunch. Jack Wiles reminds us that it's all too easy to have private conversations in public spaces, especially when grabbing a bite with coworkers. Be aware that no-tech hackers love to hang out at the corporate watering hole or food trough. So, don't fill their all-too-eager ears with company jargon and secrets.

Shred Everything

The golden rule is to shred everything. But shredding is a subjective word. There are lots of varieties of shredders, each of which provides a different level of security. While a basic shredder that churns out 3/8" strip seems decent enough, it's trivial to reassemble the pieces. Obliterating your docs with a particle shredder is nice, but those things are pretty expensive, and unless you're truly evil (or paranoid), it's just overkill.

A decent "micro-cut" shredder from an office supply store will cost around $200, and can cut paper, CD's and even credit cards into 3/32 x 5/16 pieces, for better than average security. Generally speaking, you'll get what you pay for. But whatever you

choose anything's better that putting documents in the trash in one piece, or laying them in the parking lot.

It's also a great idea to get to know what's in your trash before the bad guys do. If you're in charge of security for your company, consider at least a weekly visit to your dumpster to get a feel for what's being tossed and what condition it's in when it lands in the big green box. If you're a consumer looking to protect your privacy, get a personal shredder and have a discussion with your family members about what should be shredded before being thrown away. If your family refuses to comply, you might consider relocating them.

Get Decent Locks

Forget everything you've seen on TV—all locks are not created equal. Our experts chime in on selecting a good lock. We've already seen that many locks can be shimmed. Deviant Ollam says we can shutdown shimmers by selecting shim-proof locks. Here's his advice for selecting a shim-proof lock:

- Select a lock that can only be shut by using the key or combination.
- Select a *key retaining padlock*, which hangs onto the key when the lock is open.
- Look for "double ball" mechanism locks.
- Select padlocks which feature a *collar* or *boot* on the shackle.

This is great advice, but I found myself asking the obvious question: "Which locks do the pros recommend?" Deviant Ollam and Marc Tobias offered solid, immediate responses:

- EVVA MCS (www.evva.at/at/technology/mcs): Given the choice of one lock, both experts agree: "Give me the MCS padlock."
- Schlage Everest Primus (http://everestprimus.schlage.com): Deviant and Marc both agree: the Primus is excellent. Deviant says, "They were making a wickedly pick-resistant and totally bump-proof lock before the media had ever even caught on to the problem."
- Abloy Protec (www.abloy.com.au): Deviant says, "The company is great about refining their design to make many attacks ineffective."
- Sargent & Greenleaf 8088 and 8077 series locks (http://www.sargentandgreenleaf.com): These puppies are often found on Department of Defense filing cabinets.

Jack Wiles also weighs in, saying that the ABUS Diskus (http://www.acelock.com), which he recommends as an "odd-shaped, but all around decent" standby.

Also, keep in mind that no matter how secure your locking systems may be, you should always keep your keys out of sight of the bad guys. Barry Wels of The Open Organization of Lockpickers (Toool) reminds us that professionals can "read" a key just by looking at it, giving him a head start on either duplicating the key or picking the lock it was made for. He even reports to have heard rumors that "surveillance teams try to make photographs of keys visibly worn by suspects to give the NDE (non-destructive operator) a head start …." He goes on to say in his blog at www.toool.nl/blackbag that some prison guards "carry keys in a way the inmates can not see them." One solution is to consider a customized key carrying device like a "key port" from www.key-port.com, which conceals the keys from view, but makes them simple to take out when they are needed.

Jack Wiles also suggests some sound physical security advice:

- Check all locks at work and home, and report or fix any that are malfunctioning.
- Don't prop doors open, and report any that you do find propped open.
- Get all your locks re-keyed when you move into any home, and when you suspect that someone has been inside.
- Always consult a professional to evaluate the physical security of your home or workplace.

Put that Badge Away

Like Doris "Mama Soul" Troy used to sing, "Just one look, that's all it took, yeah just one look." This oldie's hook is like a no-tech hacker's anthem. One look is all a no-tech hacker needs to memorize, duplicate, laminate, infiltrate and frustrate. Put that badge away. It really is that simple.

Check Your Surveillance Gear

If you can bypass your own security cameras and motion sensors, a bad guy can too (and probably already has). Test out all your surveillance gear, and consider the following advice:

- Better quality cameras are less susceptible to bright light attacks.
- Domes and films can deter flaring attacks, but remember that any optic treatment can block light the camera relies on, like the infrared light used by low-light cameras.

- Use multiple cameras with fully overlapping views.
- Consider armored housing and protect the camera's video feed and power source from physical attack.
- Hidden cameras never hurt, especially when mixed with more obvious units.

Shut Down Shoulder Surfers

Watch your angles. Remain aware of the angles that shoulder surfers rely on. Don't put yourself in situations that invite shoulder surfers. Position your back to the wall when using your machine, and never leave it unattended. Don't wear company logos and remove extraneous markings and information from your mobile computing devices, especially if your company name might entice an adversary. The tech support folks in your shop can probably provide you a long list of tech things to avoid when traveling. Follow their advice.

Keep those digits to yourself. What's the point of any kind of pass code if you enter it in plain site of everyone? When entering sensitive data, create some sort of barrier between the keys and wandering eyes. This might require you to reposition your body, or create a shield with your spare hand. If you aren't willing to do this, why have a pass code at all?

Throw down! I'm not suggesting you body tackle every oddball that might be shoulder surfing you. What I would suggest is that you close your laptop (or turn off your monitor) if you think you're a target and become suddenly (and obviously) interested in something else, like sipping your coffee. Most no-tech hackers will know they've been busted and move along. If they do bail, keep a casual eye on them as they leave and try to get a good look at them and their car/bike/skateboard/Segway before they bail. When they've cleared out take a look at what you were working on, consider all of it compromised, and act accordingly. If your surfer doesn't bail after you close your lid, keep an eye on him or her anyhow. If he or she continues acting suspiciously, do something about it. Inform a manager, security guard or hall monitor. Do *something*. If that something involves physical violence, just don't tell the judge it was my idea.

Block Tailgaters

Don't let them in. If someone you don't recognize attempts to tailgate behind you, slam the door on their wanna-be hacker fingers. That will not only keep them out of your building, but will also put a serious cramp in their Google-hacking mojo. If they

turn out not to be a hacker, apologize and take them out for lunch. Be nice and make it a place with some one-handed fare—fast food joints offer a great selection. Strangers will come to fear you, but the security goons will love you, and that's important.

Err on the side of caution. Don't settle for taking the world at face value. Too many people see a logo or a uniform and make bad assumptions. Don't be that person. If your Spidey-sense tells you something's wrong, it probably is. If you don't have Spidey-sense, walk loudly and carry a big stick. Whatever you do, don't let the security of your home or workplace rest on poor assumptions.

Quit Smoking. I love smoking entrances. They are my preferred method of entry to even the most secured facilities. So either quit smoking, buck the system and just smoke in the office, or remember that the stranger hanging outside with you might just be me.

Policy rhymes with "juicy," kind of. Policies are good. As Jack Wiles shares, "Unless there is a strong corporate policy requiring all employees to challenge anyone that they can't identify, [tailgating] is a difficult problem to deal with. At an absolute minimum, employees should be trained on when and how to notify security if they suspect that an unauthorized person has followed them in."

Clean your Car

Stickers are not your friends. No-tech hackers can tell an *awful* lot by checking out your car's stickers. If you don't absolutely need them, take them off. The worst offenders are oil change stickers, parking permits and membership stickers. Some required stickers don't need to be permanently attached. If you can get away with it, mount the sticker to an index card, and store it behind your visor when you aren't using it.

Get rid of that junk. Remember the old adage of the eight P's: "Printouts, paychecks, personal and private papers persuade peeping people." So it's not exactly wisdom of the ages, but I guess it works. That junk in your car might be much more than an eyesore—it might provide information that a bad guy could use to profile you. Prevent profiling by practicing proper pick-up. And avoid a pithy saying battle when your opponent is armed with a thesaurus.

Play it smart, G-Man. Government parking permits on cars in the parking lot indicate a government facility is nearby. Be extra vigilant if you work in a building that contains a large number of these permits, and be on your guard as the building may be the target of an attack in the form of a tailgating, social engineering, dumpster diving exercise—or worse.

Watch your Back Online

Avoid Instant Messaging profile pitfalls. We could do an entire book on the privacy implications of using instant messenger (IM) programs. When you sign up for a new IM user account, most services create all sorts of personal data trails that a hacker or identity thief could uncover. Never enter personal information about yourself that you wouldn't give to a personal stranger. Also, make sure your client is set to confirm every action a remote user might take such as uploads, downloads and requests for profile information. Poorly configured IM clients are bad news if you're concerned about your privacy.

Keep an eye on P2P software. It's scary to think about a hacker targeting your personal information, but understand that P2P hacking is not about targeting specific individuals. P2P hacking is about finding interesting information based on specific keywords. If a hacker's after you, he or she is probably not going to log into a P2P client in search of your information because this makes the assumption that you're running a P2P client *and* that you have shared personal data there. Both of these are rather wild assumptions. So if you do run P2P software, make sure you know exactly what it is you are sharing, and then make sure your personal firewall, and virus/spyware/adware software is current and correctly configured.

Google yourself. Even if it's not your fault, your personal information can end up landing on the Web. If it gets on the Web, Google will crawl it. If Google crawls it, your stuff's open to the low-tech hacking techniques of Google hackers. Googling yourself is never a bad idea, but remember that Googling an entire credit card number or all the digits of your social security number is a bad idea—the search term itself then becomes private data. Instead, search for your name and address, or a portion of your name along with a portion of a sensitive number. Better yet, use the *numrange* operator to search for your name along with a range of numbers *around* those sensitive digits. For more on advanced searching with Google, I've heard that *Google Hacking for Penetration Testers* from Syngress publishing is pretty decent.

Beware of Social Engineers

It's not about the giving. For a social engineer, it's about getting something. You might not know when you're being conned, but whenever a stranger elicits sensitive information from you, it's a distinct possibility.

Stay constantly aware. "Every unknown voice on the phone is a potential Social Engineer," says Jack Wiles, "until I feel otherwise. I'm not paranoid, just careful."

Get into a program. If you're in charge of security for your company, Jack suggests you conduct social engineering awareness training explaining how to avoid becoming a victim. He goes on to say that security awareness training is the overall least expensive and most effective countermeasure that you can employ in your security plan. He also suggests role playing as a way of showing what social engineering looks like, and social engineering "tiger team" attacks that focus on uncovering and revealing weaknesses and sharing lessons learned with employees.