Philip Alexander

Home and Small Business Guide

to Protecting Your Computer Network, Electronic Assets, and Privacy

Home and Small Business Guide to Protecting Your Computer Network, Electronic Assets, and Privacy

This page intentionally left blank

Home and Small Business Guide to Protecting Your Computer Network, Electronic Assets, and Privacy

Philip Alexander

PRAEGER

Westport, Connecticut
London

Library of Congress Cataloging-in-Publication Data

Alexander, Philip, 1963–
Home and small business guide to protecting your computer network, electronic assets, and privacy / Philip Alexander.
p. cm.
Includes bibliographical references and index.
ISBN 978–0–313–36007–7 (alk. paper)
1. Small business—Computer networks—Security measures. 2. Small business—Data processing—Security measures. 3. Computer networks—Security measures. 4. Computer security. 5. Database security. I. Title.
HF5548.37.A438 2009
005.8—dc22 2008046773

British Library Cataloguing in Publication Data is available.

Library of Congress Catalog Card Number: 2008046773
ISBN: 978–0–313–36007–7

First published in 2009

Praeger Publishers, 88 Post Road West, Westport, CT 06881
An imprint of Greenwood Publishing Group, Inc.
www.praeger.com

Printed in the United States of America

The paper used in this book complies with the
Permanent Paper Standard issued by the National
Information Standards Organization (Z39.48-1984).

10 9 8 7 6 5 4 3 2 1

Contents

This page intentionally left blank

Preface

They're out there: data security books, written to make computer systems harder to hack. Most are written in that secret language known only to computer engineers. I've heard terms, including *techno-babble* and *engineer-ese* to describe how engineers appear to speak in tongues when overheard by non-computer-savvy people. That certainly applies to books like these—but not this one. There are also myriad resources for people trying to obtain any one of the dozens of data security certifications available in the industry today. These books are all well and good; but then again they are geared towards either the computer engineer or the information security professional, not to the general public. I must plead guilty, as I have also written books and articles for that audience.

It's time for a book on data security that the average computer user can understand. I've seen it time and again: people get frustrated because they don't know if their computers are secure or even working properly. Most people, for example, want to keep the personal information stored on computers safe. They know the hackers are out there but aren't sure how best to protect themselves, their computers, and the data stored therein. The problem is that to many, the computer is such a mystical black box, that they don't even know where to start or what questions to ask. In frustration, some chose to go to the non-techno extreme, and live "off the grid" so to speak. They don't have e-mail accounts, and they don't surf the Web for fear of being hacked. They might not even use credit or debit cards to reduce the risk of identity theft. While these measures certainly will work to a point, they are not the silver bullet one might think they are. Whenever we go see a doctor, get a prescription filled, obtain a driver's license, or apply for a job, we give people information about us. Information that, if not properly safeguarded, could expose us to the risks of identity theft. In some cases, there's not much we can do. But a variety of simple steps, which this book describes, can increase the security of our home or small business computer systems manifold.

I've also been heartbroken when I learn of a friend who has been taken advantage of by unscrupulous salespeople tricking them into buying far more equipment and software than is necessary in order to make full use of their home and small business computers. While I have long been instinctively aware of the need for a comprehensive resource for the non-computer geeks out there, it never dawned on me to write a book on the topic. Until now.

It has often been said that some of our best inspirations come from having discussions with our friends. Well, in this case, it is certainly true, for it was while discussing with a couple of my friends the release of my second book, *Information Security: A Manager's Guide to Thwarting Data Thieves and Hackers,* that we touched on the need for a similar guide for average users. Soon thereafter, I was asked to consider writing a data security book for the general public, one geared to small businesses as well as owners of home computers. In other words, a data security book for the rest of us.

This book contains straight talk for those concerned with safe practices for everyday computer usage as well as data security issues. I'll talk about ways to protect your small business computers and electronic data. Arguably, small businesses can be at a greater risk if their computer systems are lost, since they often don't have elaborate backup plans like big businesses do.

I will also discuss tips and tricks on how to protect home computers, whether for personal use or for that home-based business. I've provided some guidelines on how to safeguard your personal information when purchasing items online. As a parent, I'm also keenly aware that the Internet can be an incredible wealth of information. My two sons regularly use it to help with their schoolwork. However, the Internet can, unfortunately, also be a very dangerous place, frequented by—or perhaps I should say infested with—child predators. So, as one parent to another, I've included some tips on how to help protect our children. Because cell phones, PDAs, and other mobile electronic devices have security issues as well, I will discuss methods for keeping data safe and secure. Tips and tricks on how not to become a victim of identity theft? You bet—that's in here too.

Most importantly, I cover ways to keep our kids safe while they're surfing the Internet. Whether it's cyberbullying, online predators, or just plain "stranger danger," the Internet can be as dangerous as it is informative.

Here is my promise to you: You will find no strange computer jargon that goes into elaborate discussions about, for instance, the differences between any-cast and broad-cast network traffic. I'll keep out of this book any of the vernacular spoken amongst computer security professionals but not commonly used by the general public. Bottom line: You'll get plain-English, non-techie advice on how to keep your computers running and your data safe in this high-tech world that we live in.

We have a lot of ground to cover, so let's get started.

Acknowledgments

As I'm finalizing what is now my third book, I must admit to still experiencing a certain degree of disbelief. If anybody would have told me 10 years ago that I would be a published author, I would have laughed. Then, while sitting at a presentation discussing the current state of data security compliance, the idea for my first book came to me. What is now what I realize to be reverse order—I wrote the book first, and then tried to find a company that would agree to publish it. I have also learned that if you thrive on rejection, try to become a published author. Of the more than a dozen publishing companies that I approached, most didn't even acknowledge me. The rest all turned me down, except for one, of course. As the saying goes, lightning only needs to strike once to get lucky, and hence my first book, *Data Breach Disclosure Laws—A State-by-state Perspective* was born. The experience also told me to follow your dreams. You will never know what you are capable of if you don't try. If you have a dream a writing a book yourself, go for it.

This leads me into wanting to acknowledge the publisher of my next two books, Greenwood Publishing Group, and especially my editor Jeff Olson. Jeff was one of the editors that I reached out to trying to pitch my first book. Jeff contacted me and asked if I could write a book on information security at a broader level, targeting compliance officers, senior executives, information security officers as well as risk officers. Almost a year later my second book, *Information Security: A Manager's Guide to Thwarting Data Thieves and Hackers* hit the bookshelves. Now fully into the groove of writing, I had an idea to write a computer security book aimed at helping the general public. I pitched the idea to Jeff, and lo and behold, here we are with what is now my third book. So, I want to extend a personal thank you to Jeff for working with me.

I also want to acknowledge both my Uncle Max and Aunt Myrna. I believe that every boy needs a strong male figure to help guide him through the journey of life and make the transition from childhood to becoming a man. If you're lucky, that person will be your father. It was my father for me until he passed away when I was 25 years old. While no person could ever replace my dad in my heart, my Uncle Max has been like a second father to me, always there to offer the fatherly advice that I have come to value so much even into my forties. Thanks, Uncle Max—you're the best. My Aunt Myrna has always been there for me was well. She is always supportive, and the high opinion that she has of me is humbling. I only hope that I can be the person that my Aunt Myrna believes that I am.

I also want to thank my wife Cency and our two sons Freddy and Danny. Writing a book takes a lot of time and energy. It's time and energy that was not spent on them. While I always tried my best to take time out to be the good husband and father, I must acknowledge their sacrifices, as well. I spent long hours conducting research and writing the formation of this book. It's time that I didn't spend with them. So, to quote a line that many professional athletes have used in the past, "Pack your bags kids, we're off to Disneyland."

Chapter 1

Job #1: Secure Your Network

Experts in the field of computer data security often state, and correctly so, that there are no silver bullets when it comes to securing a computer network. No one piece of hardware or software exists that will secure your computer and the data contained in it, from all evils that can possibly affect it. This would include things such as malware—a fancy word for computer viruses as well as other kinds of malicious software—and, of course, attacks from hackers. For medium-to-large companies with expansive computer networks, that statement is absolutely true.

However, in this case, I'm not talking about large computer networks. The focus of this book is centered on securing computer systems of a much smaller scale. This could mean a small business, a home-based business, or even the computers in your house. These computing systems are mainly used for e-mailing, surfing the Web, storing the pictures that you've taken with your digital camera, and performing research for a school project.

Securing a small computer network is akin to locking all the doors and windows in your house. Once done, a certain degree of security has, in fact, been obtained. Conversely, trying to lock all the doors and windows in every house and every business in a large city such as Chicago or New York would be incredibly difficult. Just as there are fewer doors and windows to lock in a single house, it is also easier to secure the computers that are just used either by your immediate family or by a handful of employees, than it is to secure a network used by tens of thousands of employees in a large company.

Hackers and Why They Hack

Hackers are motivated by different things. It's akin to asking why people commit arson. Some do it to try to collect on the insurance money, while others have a mental disorder that compels them to commit arson. Then, there are others that burn down homes out of a sense of social justice if the structure is built in an area that they believe should be left undeveloped.

Whatever the motivation, the end result of an arsonist is the same: fire damage to various degrees. The same is true with hackers. While their motivations may differ, the end results of hacking are generally the same. Your computer doesn't work as it should, your data is stolen—or in some cases, it's a combination of both. Large companies are often the specific target of hackers. A company may be involved in a business that is politically divisive and that invites the ire of people who don't share the same view. Potential hackers could deem the company to be either socially or environmentally irresponsible. Whatever the reason that the perpetrator uses to justify the activity, the act of being a hacker activist has been labeled "Hacktivism." Hacktivists are comparable to the aforementioned arsonists that burn down homes built in places that they feel should be left undeveloped.

Sometimes hackers target businesses due to the nature of the data that they collect. Businesses that accept credit cards as payment for their products and services are often the target of those trying to steal information in order to commit financial fraud. Just having personally identifiable information, such as Social Security numbers, on a network will attract hackers intent on committing identity theft.

Sometimes, the only reason a hacker will choose a target comes down to simple bragging rights. This is the hacker who is looking for the right to be able to post the fact that they just hacked a famous company's computer network on a hacking community Web site.

While home computers and small business computing networks certainly pose less of a target, they certainly are not risk free. Whether it's a novice hacker trying to better hone his skills, or a more seasoned one wanting to take over your systems for some nefarious purpose, small networks are at risk from hackers as well.

LIMIT PHYSICAL ACCESS TO YOUR COMPUTERS

Large companies take elaborate measures to control the physical access to their servers. It is not uncommon to have entire buildings specifically designed to house servers and, as such, to contain a huge number of physical security controls. Such buildings are referred to as data centers. A common security measure is the presence of an around-the-clock uniformed security guard, on site 24 hours a day, 7 days a week. In addition, employees are generally required to display a special photo identification badge at all times. Often, that badge has data imprinted on it, in a fashion similar to the magnetic strip on a credit card. The data will let them gain access to certain areas of the data center, while denying access to other areas. The badge may also limit the times when an employee can access the building. The heart of the data center itself may very well require some sort of biometric authentication such as a fingerprint in order to gain entry. Even if an employee can get into the same room with the servers, the servers will be in locked cages. To be able to actually get to the servers themselves, the employee has to be authorized not only to be in the server room, but also to be able to check out a key to a particular cage containing the servers he is trying to access. On top of that security, it is common for server rooms to also be equipped with closed-circuit television cameras, which monitor the entire building and record his every move.

While a small business with a handful of employees is not going to have a dedicated data center, controlling physical access to the computers that you use for your small business is very important. If you allow a hacker physical access to a server, the question becomes not whether or not they will be able to break into the system, but when. The same goes for workstations and laptops. There are steps that can be taken that are neither as grandiose nor as expensive as the aforementioned data centers. Placing your computers in a locked office at your place of business is a more secure solution than putting them in an area that is frequented by customers or delivery people. Consider your computers to be sensitive equipment, and try to limit their exposure to the general public. If your employees' job descriptions do not require the use of a computer, don't leave your business's computers where employees could access them. Treat your computers as you would treat your employees' personnel files.

There is also something to be said for the concept of "security by obscurity," similar to the concept of *out of sight, out of mind.* Just by keeping your computer out of plain sight, you will reduce the chance that somebody will try to "tinker" with it. Instead of placing it in a highly trafficked area in your place of business, keep it in your office. Put your computer in a place where only those with a legitimate need to access it can. Employees with no business need to sit at the desk in your office are less likely to mess with your computer that is in there as well. Locking your office door when you leave will not only help protect your computer, but also other items that you have in there. That includes business plans, personnel files, customer lists, invoices, and anything else that you wouldn't want your employees to see.

Over the span of my career (20 years and counting), I have seen computers located in some crazy places. I have seen brand-new computers, still in their boxes, propping open doors in desolate areas in the dead of night. That is almost like sending out an invitation to steal them. When I expressed my concern, I was told that since there was no data on the computers yet, it was no big deal. In my mind, that kind of mind-set is akin to locking car doors only when it holds something of value. If you think for a moment, you should realize that aside from the passengers, the car itself is likely more valuable than anything inside it. An unlocked vehicle is only inviting car theft. Even pre-owned cars today can cost well in excess of $10,000, on average. Doesn't it make sense to try to protect them? How many people carry $10,000 in cash with them?

I once worked as a computer repair technician traveling to a very remote area of northern Arizona. This particular company had placed their server in the men's bathroom. I literally had to sit on the toilet in order to work on the computer. This most certainly was not the high point of my computer career. Aside from the obvious lack of physical security, you can imagine this system was not protected very well from the elements. (I'll spare you the specifics.)

PROTECT YOUR COMPUTERS FROM THE ELEMENTS

Take care not to place servers, or even workstations or laptops, in places where they may be exposed to rain, dust, moisture, or other elements that can get them dirty and cause them to malfunction. I have seen computers placed in areas where the ventilation was so bad that the entire inside of the computer was crammed full of dust bunnies. Think about what happens to your vacuum cleaner when the bag gets too full. Just as a clogged vacuum cleaner won't operate properly, a clogged computer can fail as well. In one convenience store, a computer was placed dangerously close to the soda fountain. Soda is far too syrupy and sticky to be a good neighbor for computers.

It is also important to protect computers from extremes of either heat or cold. A computer's hard drive spins at speeds of up to 10,000 times per minute, depending on the model. That can generate a fair amount of heat. Computers can easily burn out if not given sufficient ventilation or if exposed to high enough temperatures. A frozen computer isn't much better than an overheated one. So make sure that your computers get adequate ventilation, and protect them from extremes of either heat or cold. Obviously, rain, sleet, and snow won't do a computer any good, either.

COMPUTERS AND ELECTRICITY

You can take other measures to protect your computers, whether at home or in your business. Make sure that they have a good, clean source of electrical power. Computers react badly to fluctuations in electricity. A good way to protect computers from sudden unexpected spikes in power is to use a surge suppressor. Many surge suppressors can also act as a power strip and accommodate six or more electrical devices. They are relatively inexpensive, and you can get them at electronics stores, computer stores, and even stores like Target and Wal-Mart. I recommend surge suppressors not only for your computers, but also for your televisions, stereo components, or any other piece of electronics you want protected from an expected surge of electrical power. They are a small investment that offers your computers and other expensive electronic equipment a good degree of protection. Also bear in mind that a spike in electrical power can damage a computer's hard drive, which could potentially result in data loss.

Computers react very badly to a sudden loss of electricity such as a power outage—what is commonly referred to as a blackout. While laptops have internal batteries, servers and workstations do not. You can purchase external batteries specifically designed for computers that are called Uninterrupted Power Supplies, or UPS devices. Smaller ones are fine for home systems, and you can use slightly larger ones for your business. UPS devices are designed to allow you the time you need to gracefully power off your computers so as to avoid losing data, and to avoid other technical problems caused by a power failure. They generally are not designed to act as an alternative power source that allows you to continue working. So if the power goes out, shut the computers down.

If your business model requires that your computers stay on even with a loss of main power, you'll have to obtain a reliable source of alternative energy. This could mean that you have a sufficient quantity of UPS devices to allow work to continue. However, a more common alternative form of electric power is a diesel-powered generator that can provide backup power until the main power is restored. Investing in large diesel generators and accounting for a sufficient amount of fuel to keep them running is not a cheap endeavor. Like many measures to protect computers, it should be a business decision predicated on your specific needs. If generators do fit into your business model, you will definitely want to invest in surge suppressors for your computers. Diesel generators are far more prone to power spikes than is a city's power grid.

Greater Access = Greater Risk

An unfortunate truth is that while providing your computers a degree of physical protection is important, the majority of hacking attempts are undertaken by people not located anywhere near them. That's because today's risk model is much different from what it was in years past. When computers first started to appear in offices and in the home, they were isolated systems.

There were no Internet or wide area networks. Computers were mainly used for word processing and for playing games such as Minesweeper and solitaire. It simply was not possible for a hacker located on the other side of the country, much less one located abroad, to gain access to a system that had no connectivity to the outside world.

I can remember when file sharing meant copying data to a floppy disk and walking it over to a coworker, who would then load the file onto their computer. The colloquial term used for that kind of file sharing was called "sneaker net." Even when the Internet first appeared on the scene, the risks to computers were still relatively small. That was because in the "old days," people used dial-up modems to gain access to the information superhighway. By today's standards, dial-up modems are painfully slow. Furthermore, back in the modem era, most computers were only connected to the Internet when users were actively online. Contrast that model with what we have today. Digital Subscriber Lines (or simply DSL) and cable modems are light years ahead of old-style dial-up modems in terms of speed. They are both also "always on." That combination of high speed and near-continual access has made the job of hackers and others who would use the Internet to cause mischief and harm much easier.

TURN IT OFF: AN EASY HACKER PROOFING TECHNIQUE

There is a saying in computer security that there is no such thing as making a system "hacker proof." The underlying assumption behind that statement is the supposition that the computer systems must always be powered on as well as connected to the Internet. That is actually true for businesses that sell their products and services online. Their Web servers are up and running around the clock, and hence are always a target for hackers. Consider the fact that companies like eBay and Amazon.com can't very well turn their computers off at night. That said, we are not all eBay and Amazon.com.

If you don't need your computer to be connected to the Internet all the time, then disconnect it. A computer that is not connected to the Internet is next to impossible to hack remotely. The same strategy will work for businesses as well. If your business computing needs do not require that you always be connected to the Internet, then don't be. With this simple approach, you will stop hackers cold. I often advise people that computer security risks can be thought of similarly to other risks in business. Consider the fact that every time a bank sells a mortgage, they are accepting some risk. The mortgagee can default, costing the bank money. The bank performs due diligence to make an informed decision about whether or not to loan the money to a particular customer. They will ask customers to provide information about both their income and expenses. The bank will also perform a credit check to see if the customer has a history of paying their bills on time. The bank will perform these checks to see if the benefits of selling the mortgage, i.e., the interest payments on the loan, outweigh the risks. The same cost-benefit analysis can be applied to risks involving computers. If the benefits, either to yourself or your business, don't outweigh the risks, reevaluate the situation.

In short, if you do not need to be connected to the Internet, then don't be. If you are not aware of the potential risks you might be accepting, then I humbly submit that you are reading the right book. Since the best decisions are always well-informed ones, read on.

There is an even more powerful technique that will thwart data thieves and hackers than disconnecting your computers from the Internet. For both home users and businesses alike, perhaps the most effective anti-hacker tool is to simply turn off your computers before you either leave work for the day or go to sleep at night. During the day, if the kids are at school and you are at work, don't leave your home computers on and connected to the Internet. When you shut your doors at the end of the business day, if you don't need your computers to be on, then turn them off. Not only are you saving your computers from the dangers of hacking, but you are also saving money. Whatever else computers are, they are also electronic devices. Just as you would turn off the television or the radio when not using them, consider turning off your computer as well.

I can almost hear the protests of many of my readers now. They will say, "I need to leave my computer on, at least during the day because it takes too long for it to power up, and that is just inconvenient." Not to worry; there are techniques that you can use to stop hackers that don't include powering off your computer. Hackers need your computers to be powered on *and* connected to the Internet in order to try to perform their mischief. If you were to power off either your cable modem or your DSL connection, that would take your computer off-line, and again stop hackers cold. Both cable modems and DSL connections generally power on much more quickly than computers do, so it would be less of an inconvenience to wait for them to be ready to use again. So, if you are either not using your computer at the moment, or using it but don't necessarily need the Internet, go ahead and go off-line.

There are also ways to take your computer off-line, disconnected from the Internet, without powering anything off. While they are discussed in more detail in Chapter 7, most brands of personal firewalls have a simple on/off setting that is designed to stop all Internet traffic. While they are not as foolproof as powering off your computer or cable modem, bear in mind that the overwhelming majority of Internet hackers are not targeting you specifically.