OWN YOUR SPACE

Compliments of Microsoft

Protect Your Turf

KEEP YOURSELF AND YOUR STUFF SAFE ONLINE

Edited by Linda McCarthy and Denise Weldon-Siviy

The author and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein. All trademarks are the property of their respective owners.

Publisher: Linda McCarthy
Editor in Chief: Denise Weldon-Siviy
Managing Editor: Linda McCarthy
Cover designer: Alan Clements
Cover artist: Nina Matsumoto
Interior artist: Heather Dixon
Web design: Eric Tindall and Ngenworks
Indexer: Joy Dean Lee
Interior design and composition: Kim Scott, Bumpy Design
Content distribution: Keith Watson

The publisher offers printed discounts on this book when ordered in quantity for bulk purchases, or special sales, which may include electronic versions and/or custom covers and content particular to your business, training, goals, marketing focus, and branding interests. For more information, please contact:

U.S. Corporate and Education Sales
(510) 220-8865

ISBN 978-0-615-37366-9
Library of Congress Cataloging-in-publication Data

McCarthy, Linda
Own your space : keep yourself and your stuff safe online / Linda McCarthy.
ISBN 978-0-615-37366-9 (electronic) 1. Computer security. 2. Computers and children. 3. Internet and teenagers. 4. Computer networks-Security measures. I. Title.

Visit us on the Web: www.100 pagepress.com

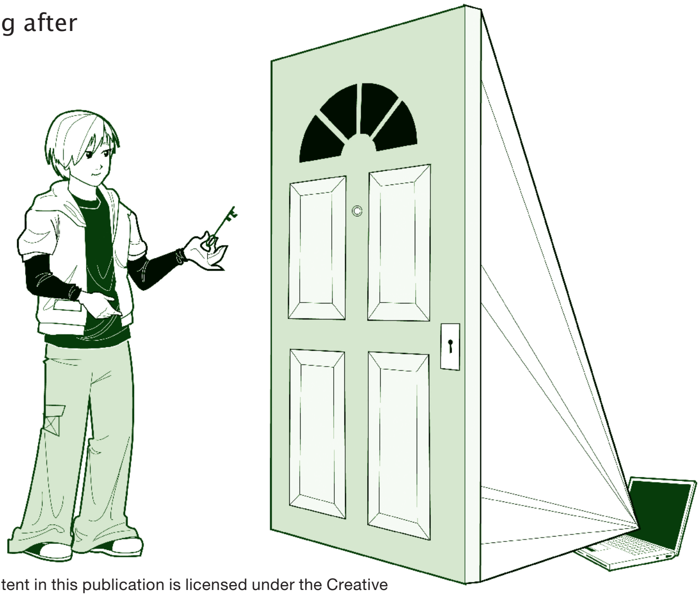
Download free electronic versions of the book from MySpace (http://www.myspace.com/ownyourspace)
and Facebook (http://www.facebook.com/ownyourspace.net),
and from Own Your Space (http://www.ownyourspace.net)

rev 2.0

Chapter 1

Protect Your Turf

Braden is a typical 14-year-old. Over the past 6 months, he's grown three inches, gained four shoe sizes, and eaten his way through nearly a ton of pizza. He's also unintentionally trashed his family's computer no less than 12 times. First, he downloaded some cool emoticons to use with his IM messages. Those smiley faces came with embedded adware that overwhelmed him with pop-up ads and slowed down the speed of virtually everything. Then Braden installed a "free" video game that contained a Trojan program that let spammers in Russia take over his computer and use it to forward junk email. A few weeks later, Braden responded to what looked like a legitimate email asking him to confirm his Facebook login information. That phisher then used Braden's login to post links to adware to Braden's Facebook friends. Not long after that, Braden clicked **Yes** to install security software when a pop-up announced that his computer was infected with adware. As you've probably guessed, that software installed more adware. Braden's mom has spent so much time, and money, having the family computer fixed that she's beginning to wonder if the Internet is really worth the aggravation. What she is sure of is that Internet security has become a LOT more complicated than it used to be....



ISBN 978-0-615-37366-9

Since the Internet's inception in the late 1970s, the number of people who use the Net has doubled every 9 to 14 months. Do the math and you'll see a phenomenal growth chart—from 281 computers on the Internet in 1981 to a dazzling 400 million in 2000. By 2009, worldwide usage passed 1.5 billion **netizens**. Internet usage in the U.S. is nearing saturation levels.

Netizen A citizen of cyberspace (i.e. the Internet). A netizen is any person using the Internet to participate in online social communities. When you confirm a new friend on Facebook, you are expanding your online social group. You are being a good netizen!

While Internet usage among adults has risen steadily, Internet usage among teenagers has soared. As of June 2009, 90% of American teens lived in homes with Internet connections. If you're part of that 90%, it is especially important for you to understand how to protect your computer from nasty code.

As you'll learn later, your computer is at special risk. Adware sites target teenagers just like you by focusing their efforts on websites you and your peers tend to visit. Online forums are targeted by pedophiles posing as teens. Even identify theft, another potential consequence of nasty code, can be especially nasty for teenagers still in the process of defining their financial and business identities. If you use your parents' computers, you may also put their financial and personal information at risk.

For now, just keep in mind that there's a lot more to Internet security than running antivirus software. And, it's a lot more important than you probably realize. Over the next few chapters, we'll talk about what you need to know and do to help keep yourself, your computer, and maybe even your parents safer when using the Internet.

1.1 A Survey of Malware

Malware is a generic term for a piece of malicious code. That is, programming code specifically developed to harm a computer or its data. If you've studied Spanish (or Latin, for that matter), you'll know that "mal" means bad—like malcontent (an un-contented, unhappy person) or Darth Maul in *Star Wars Episode I* (the obvious bad guy dressed in red and sporting horns). Nothing good ever starts with "mal." Malware is, quite literally, bad software.

Malware Programming code designed to harm a computer or its data.

Since malicious code and malware mean the same thing, for simplicity's sake we use the term malware throughout this book.

In the world of malware, there are several standard types of villains. We'll be covering all of these villains throughout the book, but the main categories are

- Viruses
- Worms
- Trojans
- Bot armies
- Keystroke loggers
- Spyware
- Adware
- Scareware
- Ransomware

You're probably already familiar with some of these categories. For instance, computer viruses are now so well-known in the popular culture that they provided the grand finale to the 1996 sci-fi thriller *Independence Day*. If you'll recall, Will Smith saved the day by helping Jeff Goldblum (better known as Ian Malcolm of *Jurassic Park*) to upload a computer virus to the "mother ship," disabling the alien space crafts' force fields. In real life, viruses and worms have taken out entire unprotected networks. In August 2009, attackers shut down Twitter for nearly three hours, leaving 44 million tweeters worldwide out of touch. If that doesn't sound like a big deal, imagine CNN or Fox News being driven off the air for an afternoon.

You are no doubt also familiar with antivirus software. Most, but not all, new computers now arrive fresh from the factory already preloaded with at least a trial version of one of the major antivirus packages. Usually, that's Norton AntiVirus, Trend Micro, McAfee, or Webroot. For virus protection, they are all excellent products.

You may not be aware, however, that antivirus software can't protect you against *all* types of attacks. Many people think as long as they have antivirus software installed that they are protected. That's not true because several layers of security are needed to protect you. Antivirus software is only one of those layers.

Before we take a look at the other layers of security, it is important to understand what antivirus software can and cannot do. Think of your antivirus software as a series of vaccinations. Having a polio vaccination won't keep you from getting hepatitis. Likewise, having antivirus software won't necessarily protect your computer from spyware or adware. In fact, if you don't routinely update your antivirus software, it may not even protect you from viruses. Like their biological cousins, computer viruses mutate. Just as you may need a new flu shot each winter to protect against new viral strains, you also need to update your antivirus software continuously. For other types of malware, you may need other types of protection. We'll explain these as we discuss the specific types of malware.

1.2 Protect Your Turf, Then Surf!

When you buy a computer, it is not secure. You should never pull a computer out of the box and connect it to the Internet unless you take steps to protect it. Think of your PC as a world traveler who needs vaccinations to avoid diseases in its travels.

In fact, your new computer most likely is plagued with numerous **security holes**, which are flaws in the way your computer's programs have been written that would make your computer vulnerable to attack. Just how serious the flaws in the code are determines how much access an attacker or that attacker's malware can gain.

Warning!

Uneducated programmers + programming mistakes = security holes!

If you're wondering why your computer has holes before you use it, the answer is that computer systems run on programs—literally tens of millions of lines of code that tell the computer how to interpret what you, the user, want to do. All those lines of code are written by human programmers. Those programmers can make mistakes that can be leveraged by hackers to gain unauthorized access to your computer. This probably sounds strange, but most programmers were never taught how to write secure code. To take it one step further, programmers don't think like criminals. We don't use that term very often, but that's what someone who deliberately steals or damages someone else's data is—a criminal. Your average programmer hasn't always thought, "Gee, I could use these lines of code to break into someone's computer," because the programmer doesn't actually WANT to break into anyone's computer.

Security Hole Any flaw in the way a computer program is written or used that makes your computer vulnerable to attack. Security experts also call this a security vulnerability.

The lack of focus on security as part of the design process is starting to change. More programmers are beginning to audit (double-check) their code with special tools that look for programming errors that can lead to unauthorized access to the system or data. It will take a long time for the programming community to catch up, however. Think of the millions of lines of code already out there that have been developed by programmers with good intent, but poor security-programming skills. Since all computer systems have security holes, you must protect yourself and patch those holes before you start surfing the Internet, downloading music, or gaming.

Warning!

Once connected to the Internet, an unprotected PC can fall victim to an attack in as little as 15 seconds! Protect your PC before you surf!

Why so fast? Once you're online, it can take as little as 15 seconds for someone to attack your machine. If you don't install security first, that first attacker may gain access to your computer without you even knowing about it! At worst, the attacker could make off with enough personal data to steal your identity. If you use financial software to track the bank account you opened for college savings when you picked up that after school job, keep in mind that your data isn't just information. It could be cash as well. And just to add another twist, a hacker could even use your computer to launch an attack on other computers! For these reasons (and many more we'll get to later), don't ever surf the Internet without security patches, antivirus software, and a firewall installed.

BEST BUY®

Internet Security List:

Anti-Virus

Anti-Spyware

Personal Firewall

Security Patches

When you bought your computer, you probably started with a list of requirements: how much memory, how much disk space, what kind of graphics you'd need for your favorite games, whether you want to burn DVDs as well as view them. Before you go online, you also need a Computer Security shopping list. This list is a basic list. You should not leave any one of these items off your list. Virus protection **must** be on that list. You have to install it and configure it to update your computer automatically. You also need to install any security patches that have been issued for the operating system and the software you plan to use.

Security Patch A fix to a program to close a known security hole. Patches are routinely issued for operating systems (like Windows 7) and Internet browsers (like Internet Explorer and Firefox) as well as other software applications.

The Internet is an infinitely cool place, but so is the vampire royal court in Volterra. We think it would be great to actually visit such a place, but only if we understood the Volturi laws, knew about Aro and Jane's gifts in advance, and also brought our own immortals. The Internet is exactly like that! There are wonderful, new, and exciting things going on there—but you really shouldn't show up without knowing the risks, understanding how to defend yourself, and arming yourself with the right protection.

OWN YOUR SPACE

KEEP YOURSELF AND YOUR STUFF SAFE ONLINE

THE BOOK FOR TEENS THAT EVERY PARENT SHOULD READ!

A collaborative project to provide free security learning to teens and families online, made available under the Creative Commons Licensing, and made possible by the support of individual and corporate sponsors.

Every day, millions of American school children log on or log in and make decisions that can compromise their safety, security, and privacy. We've all heard the horror stories of stolen identities, cyber stalking, and perverts on the Internet. Kids need to know how to stay safe online and how to use the Internet in ways that won't jeopardize their privacy or damage their reputations for years to come.

Learn how to

- Kill viruses, worms, Trojans, and spyware
- Deal with cyberbullies
- Give SPAM the curb and smash web bugs
- Understand just how public your "private" blogs are
- Keep wireless freeloaders off your network
- Prevent sexting from ruining your life

About the team

Linda McCarthy, the former Senior Director of Internet Safety at Symantec, wrote the first edition of *Own Your Space*. With 20+ years experience in the industry, Linda has been hired to test security on corporate networks around the world. For the 2010 edition, Linda's expertise is backed up by a full team to provide the best security experience possible for teens and families online. That team includes security experts, design experts, anime artists, and parent reviewers, as well as a dedicated group of teen reviewers, web designers, and test readers.

General Computing

ISBN 978-0-615-37366-9
51999>
9 780615 373669

$19.99 US / $24.99 CAN

Cover design: Alan Clements
Cover artist: Nina Matsumoto
Cover illustration © 100pagepress

www.100pagepress.com

100 page press
Smart Books for Smart People®