OWN YOUR SPACE

Compliments of Microsoft

Taking SPAM Off the Menu

KEEP YOURSELF AND YOUR STUFF SAFE ONLINE

Edited by Linda McCarthy and Denise Weldon-Siviy

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

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)

Chapter 5

Taking SPAM Off the Menu

Tessa was thrilled beyond expression on Easter holidays when her Dad finally relented and let her open her own email account. She checked it 4 and 5 times a day—eager to have mail of her own. Everyday it seemed she was giving her new address to someone else—friends at school, kids from her church youth group, even new friends she'd met online. To make sure that everyone could find her, she added her name to online directories and even posted her new address on her family's webpage.

The first month or so, everything was wonderful. Tessa felt connected to the world. Then she started to hear from some of its darker inhabitants.

First, Tessa began getting boring stupid emails intended for grownups. Silly people trying to sell her stuff no real 13-year-old could possibly want. Some of them even tried to get her to sign up for credit cards. Tessa tried to get rid of the emails, sending replies to links that were supposed to remove her from the mailing lists. The number of emails just kept increasing.

After a while, the mail Tessa was getting got creepy. She didn't really understand a lot of the things people were trying to sell her, but they reminded her

ISBN 978-0-615-37366-9

a lot of that day in Health class she always tried to stay home. And again, the number of emails kept rising.

By the last week of school, Tessa was getting so much junk email that she couldn't find the messages from her friends in the pile. She gave up and quit using her email.

As summer started, Tessa's dad signed her up for a new email account. This time, he defined filters to automatically throw away the messages she wouldn't want. Now, Tessa's being very careful who she gives her new email address to.

Like Tessa, most teens are overwhelmed by email they don't want and really shouldn't have to see. The sheer number of unsolicited email messages also wastes incredible amounts of computer resources. In 2009, a Microsoft security report concluded that 97% of all email messages are SPAM. How is that even possible? Thankfully, not all of that SPAM manages to get through. For every SPAM email you pitch, your Internet Service Provider (ISP) has blocked several more before they even land in your mailbox. Unfortunately, that still leaves a ton of SPAM in circulation.

5.1 Email and SPAM

SPAM is the electronic equivalent of junk mail. That's email you didn't ask for (or agreed to accept without realizing) and almost always don't want. Some SPAM is junk email from legitimate companies trying to sell you their product. Others are junk email from less-than-respectable companies trying to do the same. Taken together, all those spammers eat up a ton of bandwidth.

5.1.1 What Is SPAM?

If you're curious, SPAM is actually a canned meat product. If you haven't had it, the taste is somewhere in between ham and corned beef. However, in computer usage the term SPAM comes from an early 1970's Monty Python comedy skit. In the skit, a couple is trying to order breakfast without SPAM in a restaurant where every meal comes with SPAM in some form. The overall feeling is that **SPAM** is everywhere, in everything, and you just can't escape it. Junk email definitely generates similar feelings.

SPAM Unsolicited email messages, also called electronic junk mail.

A surprising amount of SPAM is for products that are either clearly illegal or on pretty shaky ground. For example, a common source of SPAM is ads for online degree programs. In fairness, there are a number of excellent, highly respected online degree programs—particularly for master's degrees. However, most of these schools don't flood the net with SPAM advertising their programs. The schools that do tend to be—you guessed it—"non-accredited" universities. In evaluating any item or service you find advertised in unsolicited email, remember to "Caveat Emptor." That's Latin for "Let the buyer beware!" At the risk of being obvious, any college degree that you can get over the Internet while attending no classes and taking no tests of any kind is clearly not cool. This type of company is called a diploma mill. A diploma issued by such a school is not a real college degree. More important, using such a fake diploma to get a job or obtain a promotion is illegal.

5.1.2 Isn't SPAM Illegal?

That's a good question without an easy answer. Truthfully, some SPAM is illegal. Some isn't. It's also very difficult to tell the difference. Because SPAM is so disruptive, the U.S. Congress addressed it specifically in the CAN-SPAM Act of 2003, then reviewed and extended that legislation in 2005. So, CAN-SPAM is still in effect (and still ineffective).

Like most government initiatives, this effort was named by an acronym—CAN-SPAM actually stands for Controlling the Assault of Non-Solicited Pornography And Marketing. Its goal was to reduce the amount of SPAM by making senders legally liable. In fact, its definitions actually legalized a good bit of SPAM, leading opponents to begin calling it the "I Can SPAM" Act. What the bill did define as illegal was any unsolicited electronic messages that didn't include a valid subject line and header, the real postal address of the mailer, a clear label marking the content as Adult-only if it was, and an opt-out mechanism.

Felony First

In 2004, Jeremy Jaynes became the first person convicted of felony SPAM. During his peak, Jaynes sent upwards of 10 million messages a day, mostly for "get rich quick" schemes and various fake goods and services.

Sadly, the Virginia law under which he was convicted was later overturned—a reversal that was upheld in March 2009 when the U.S. Supreme Court refused to reinstate the law.

It didn't work. Three years after the passage of this act, SPAM had increased to comprise 75% of all email messages, and less than one half of one percent of those messages actually complied with the provisions of the CAN-SPAM Act.

Interestingly, the first person arrested under the CAN-SPAM Act was a teenager, 18-year-old Anthony Greco of Cheektowaga, New York. Overall, however, arrests under CAN-SPAM have been rare and successful prosecutions even rarer.

The big problem with CAN-SPAM is the opt-out mechanism. An opt-out mechanism is a way for the recipient to get off the mailing list. You've no doubt seen these in junk email that you've received. The general format is:

```
If you would prefer not to receive further information from Spammer-of-Your-Choice,
please reply back to this message with "Remove" in the subject line.
```

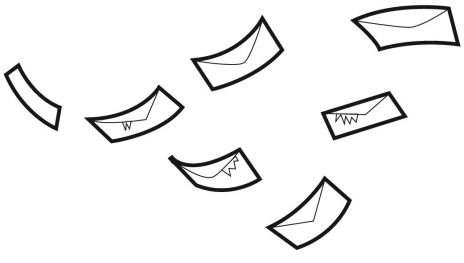
You may also have seen the format:

```
If you would like to stop receiving our advertisements or believe this message was sent
in error, you can visit our subscription management page.
```

To add more substance to their claims of legitimacy, spammers often actually cite the CAN-SPAM Act in their opt-out clauses:

```
This email is a commercial advertisement sent in compliance with the CAN-SPAM Act. We
have no desire to send you information that is not wanted, therefore, if you wish to be
excluded from future mailings, please use the link at the bottom of the page.
```

The general idea is always the same. To get off the mailing list, you need to visit the spammer's website or send them an email. The problem is that as soon as you do so, you have verified that they have a real, valid email address and that their messages are getting through. If the spammer plays by the rules, this works well. If they don't, you have just told them that your email address is worth selling. Because many spammers don't play by the rules, experts strongly recommend that you NEVER reply to unsolicited email or visit links included in SPAM. Doing so can greatly increase, rather than decrease, the amount of SPAM you receive in the future.



5.2 Spoofing

A spoof is a parody of something familiar. In its pure form, a spoof is usually a pretty good joke. Weird Al Yankovic has made a career out of writing musical spoofs of popular songs. One of his best was a 1983 parody of Michael Jackson's hit *Beat It* called *Eat It*. The music video for this one was especially funny.

Email spoofing isn't nearly so funny. **Email spoofing** happens when the person who sends you an email—nearly always a SPAM message—pretends to be someone else. Spammers are able to "spoof" messages by defining fake headers that include phony routing information. Real routing information is the part of your email that defines your email account's Internet address. These are the numbers that allow email servers to deliver your mail. You can think of the routing definition as very much like a postal address. If the address isn't valid, the email doesn't get through. Phony routing information hides the real address of the person sending an email message.

5.2.1 Spoofed Addresses

When you send an email message to someone else, the message sent always begins with a header that includes your name and email address. Those items are defined in your email software as the "Display name" and "Display email address". By changing those settings, you can actually display anything you want. Of course, tracing an email spoofed this easily would be fairly simple. Spammers also insert fake routing information; this makes it appear that the email was sent through one or more systems that most likely never touched it. Tracing messages spoofed with fake routing information is MUCH more difficult and sometimes impossible.

Spoofed email An email message containing a fake From: address making it impossible to tell where it was actually sent from.

One of the reasons that spoofing email is fairly easy is because email headers are created using **SMTP (Simple Mail Transfer Protocol)**, and SMTP lacks authentication. One way to limit spoofing is to use digital signatures with your email. We'll talk about digital signatures in *Chapter 8, Safe Cyber Shopping*.

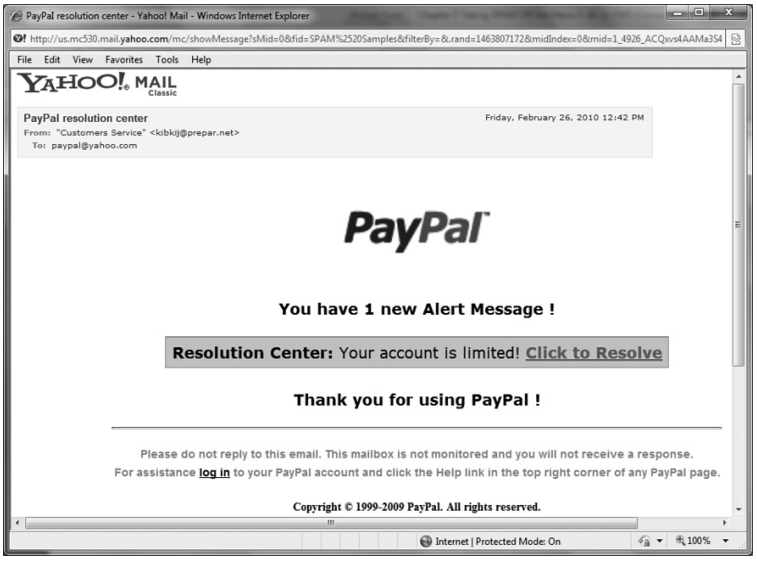
SMTP (Simple Mail Transfer Protocol) The Internet rules used to send and create email messages.

In some cases, spoofed emails are simply amusing. A few years ago, pranksters circulated a very funny election parody that appeared to all the world to have come from the Democratic National Headquarters. It was clearly a joke and the spoofing (while inappropriate) wasn't done in malice. That's not the case for many spoofed emails.

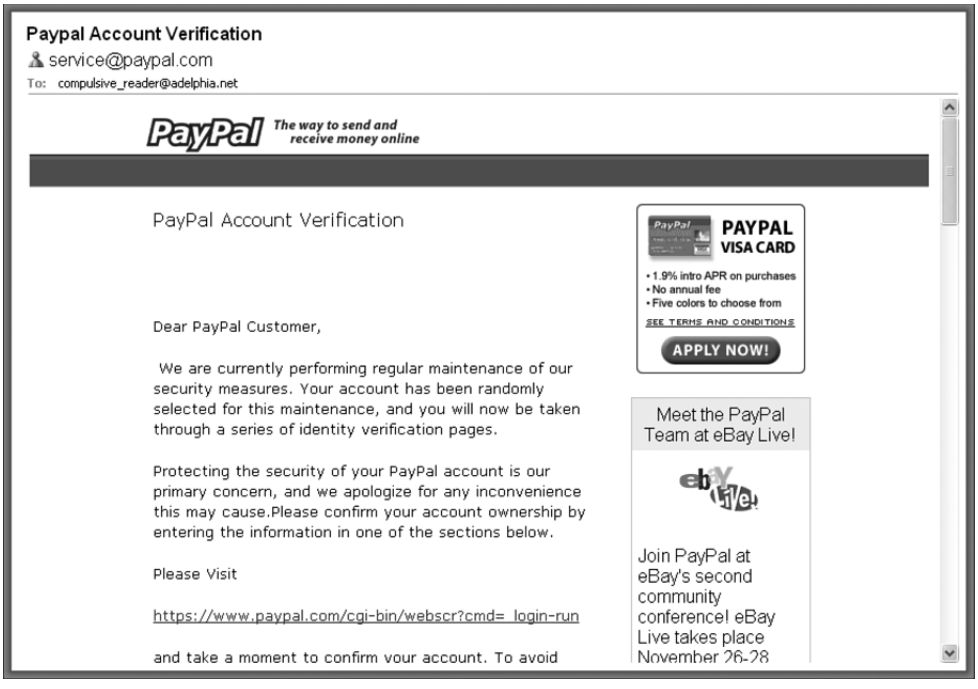
Spoofed addresses are a common theme in phishing attempts. **Phishing** (pronounced "fishing") is a con-artist trick to fish for information. Phishers send email that appears to come from a company you know and trust and asks for information that you would probably want that company to have. At the moment, users of online services like eBay, Amazon, and PayPal are often the targets of phishers. For example, if you or your parents enjoy buying items on auction at eBay, you probably have a PayPal account. PayPal allows you to create an online bank account and use that account to buy items on eBay without giving your credit card numbers to the eBay sellers.

Phishing A con artist scam to trick people into giving out personal and financial information.

If you have a PayPal account, you've probably already received an email something like this:



Or, the more detailed version:



The problem? These emails were *not* sent by PayPal. If you click the included links and enter the information they request, you will be literally giving your parents' credit card information to thieves.

We'll talk more about phishing in ***Chapter 7, Phishing for Dollars***. For now, just be aware that when it comes to email headers, what you see isn't always what you get.

5.2.2 SPAM Proxies and Relays

As you now know, much of the SPAM that is circulating didn't really come from the addresses contained in those emails. What you don't know is that some of it may even have come from your machine.

How can that happen? In Chapter 2, we talked about bot armies and how malware writers can infect your PC with a Trojan program that turns it into a zombie. A lot of those zombies are used to send SPAM. One virus that does this is SoBig.F.

SoBig also spoofs the addresses in the emails it sends so that they appear to come from someone else whose address appears in your email address book.

When a zombie PC is hijacked and used to send SPAM, it's called a **SPAM relay**. That PC is simply "relaying" (passing on) SPAM messages that originated somewhere else. This happens a lot. Unprotected home computers are a major stumbling block in the fight against SPAM.

SPAM relay A hijacked PC that's used to send SPAM without the PC owner's knowledge.

While home PCs are definitely a problem, sometimes so are the mail servers used by Internet Service Providers (ISPs). While fewer servers than individual PCs are hijacked, their extensive databases of email addresses still make them a large problem. When a mail server is hijacked to send SPAM, it's called a **SPAM proxy**.

SPAM proxy An email server that's been hijacked to deliver SPAM.

Today, ISPs are taking great care to prevent their mail servers from being hijacked. Tragically, most home PCs users are not. Luckily, the steps needed to protect your machine from being turned into a SPAM relay are the same as the steps required to protect yourself from computer viruses, worms, and Trojans.

5.3 Knock Knock— How Spammers Know You're Home

Assuming that you haven't been posting your email address all over the Internet, you may be wondering how the spammers find you and why they send you so MANY email messages. That's a good question with a couple of good answers.

5.3.1 Hidden Tracking

Popular belief has it that in the event of a nuclear meltdown, the two groups virtually guaranteed to survive are rats and cockroaches. This applies to the Internet as well. In the event of a total system shutdown, the first groups to resurface are likely to be spammers and web bugs.

If you haven't seen a **web bug**, or even heard of one, you're in the majority. A web bug (sometimes called a web beacon) is a hidden image that spammers use to track email messages. In technical terms, most web bugs are defined as a transparent GIF—a picture file having a size of only 1 x 1 pixel—making them much too small to actually see in an email.

Web bug A hidden image that spammers use to verify that you're actually reading the SPAM they sent you. (Also called a web beacon or transparent GIF.)

When you read an email message, graphics or picture elements in the email are displayed by being downloaded from a separate website. In the past, most email programs were set to automatically download graphics so readers had no idea they were downloading information from another site. Today, that default has been reset so that you'll often see broken images like this:

One by One...

When you look at a picture on your computer screen, you see a solid graphic image—much like a photograph or drawing. In reality, each computer image is composed of thousands of tiny little dots, called pixels.

The term pixel, in fact, is an abbreviation for "picture element." How many pixels a graphic has determines its resolution—how "solid" or crisp the picture looks.

If you use a digital camera, you already understand this term. A high-quality photograph takes an awful lot of pixels. For example, the Kodak Easy Share P880 provides an 8 megapixel sensor. That's eight times roughly 1 million pixels for a single photograph.

Try to imagine a picture that's only one pixel by one pixel. You can't see it, which is of course, the idea of web bug graphics.

If you click to download the graphics the spammer knows that your email address is valid and that you actually read the email message. Don't be surprised if you keep getting spammed!

5.3.2 Scavengers and Crawlers

We kidded above that you might be surprised by the amount of SPAM you get, assuming that you hadn't posted your email address all over the Internet. Amazingly, many people do just that! They use their email addresses as user names for online communities, include their email addresses on their websites, and even use their actual addresses when posting messages to online user groups. All of these steps are good ways to get SPAM.

This is also an area where it's important to lock down your social networking information. Ideally, contact information, like your email address, should be set to display only to Friends, if at all. Truthfully, you don't need to provide email addresses to anyone on social networking sites. Anyone who can find you on Facebook or MySpace can actually contact you via a message or email ON those sites without ever needing your personal address. Obviously, never include your full email address in any messages that you post to someone else's page or wall.

Email scavenger A type of web crawler program that searches the Internet and collects (harvests) all the email addresses it finds posted on web pages.

Posting your email address online can cause problems because some spammers use programs to crawl Web pages (i.e. search them) on the Internet looking for the famous @ sign which appears in virtually all email addresses. Some companies earn fairly decent profits by doing just this.

5.3.3 Is Your Email Address For Sale?

If your email address has been posted on the Internet, chances are that someone is selling it right now. Because the Net is a public place, harvesting addresses for sale (although annoying) is a perfectly legal endeavor. If you run a quick web search on "email harvester" or "email spider," you'll find a wide variety of products that harvest email addresses, most priced well under $100.

Sometimes, sellers don't need to "harvest" email addresses. They simply use their own customer or member records. In 2009, music service SpiralFrog sold the addresses of its 2.5 million customers to multiple spammers literally days before creditors took control of the now defunct firm. One of those spammers paid $8,500 for the addresses. While that was, as a former SpiralFrog customer noted, "Slimy", it probably wasn't illegal. Many free (and paid) service providers reserve the right to share, distribute or sell the information you provide them. That's why it's important for you to read each website's privacy policy before you provide that information.

5.4 Social Engineering

Strangely, some scammers focus on SPAM because people like you are beginning to get smart and protect their machines with applications that keep hackers from targeting software vulnerabilities.

Most SPAM messages rely on social engineering to trick recipients into reading the email. These are some of the same tricks that virus writers use to get you to open email attachments when you know you really shouldn't.

For social engineering purposes, spammers rely heavily on the displayed `From:` and `Subject:` fields in the email messages. Often, `From:` fields are spoofed to appear to come from companies or organizations you know and trust. The `Subject:` lines are written to catch you off-guard or play on curiosity or greed.

Here are some of the more common subject lines that spammers use:

```
Subject:  RE: About your email
```

This approach tries to catch you off-guard and trick you into thinking that this message is a response to an email you sent. Don't assume that every email that begins RE: is really a reply. Always look at the `Sender:` field.

```
Subject:  Free Xbox games for 30 days
Subject:  Sweepstakes PRIZE Notification – You WON!!!!
```

Free stuff is always great, isn't it? Since many teens enter online sweepstakes and contests, this is a very effective approach. When you receive an email like this, ask

yourself whether the prize matches up with any sweepstakes you really entered. You also might want to be careful about entering all those sweepstakes. Many exist solely to harvest email addresses.

```
Subject: Lose up to 50 pounds in one month!
```

Weight-loss SPAMs are strangely effective with young people. A 2009 study published in the *Southern Medical Journal* found nearly 20% of overweight college students actually bought weight-loss products marketed via email SPAM. Unfortunately, most products advertised via SPAM are more likely to lighten your wallet than anything else. The person to ask for weight-loss help is your doctor, not your neighborhood spammer.

5.5 Keeping Spam Out of Your Inbox

When spammers first started gaining ground, there really weren't enough good tools to keep them out. Today there are many sophisticated tools and techniques for blocking SPAM. The way you use your email address and the actions you take when SPAM gets in are both important components in keeping SPAM out.

Even though technology to block SPAM is getting better, spammers are always trying to work their way around it. No method will protect you from 100% of SPAM. Still, your first line of defense is to do the following:

- Delete suspicious email without reading it!

  This is a good way to avoid viruses and worms as well as more SPAM.

- Don't click on links in your email.

  Remember the web bugs? Don't let them crawl into your PC!

- Don't reply to SPAM.

  While a few opt-out mechanisms are really legitimate, an awful lot more of them aren't. In the long run, you'll get less SPAM if you just delete it than if you ask to be removed from the mailing list.

- Watch where you post your email address.

  To avoid being caught by web crawlers collecting email addresses, don't post your full email address on any publicly-accessible web page.

- Use filters if you have them, but don't trust them to do the whole job.

  Filters can be a useful tool in avoiding some types of SPAM. But spammers are constantly rewriting their subject lines to avoid being thrown away by filters. Often, message content is contained in a graphic/picture file. Since filters scan text, they miss any key words or phrases contained in graphics.

5.6 SPIM

SPIM is the instant messenger version of SPAM. Like SPAM, it proliferates wildly and greatly annoys its recipients.

Distribution of **SPIM** has grown with the use of instant messaging. In 2007, about 50% of American teens used instant messaging. By 2009, that figure exploded as social networking members took advantage of the IM features of Facebook and MySpace.

SPIM Unsolicited instant messages. SPIM is the IM version of SPAM.

Teens use instant messaging even more heavily than adults. As a result, they are even more likely to receive SPIM. Sometimes, that SPIM is even intentionally targeted at teens. In February of 2005, an 18-year-old New Yorker, Anthony Greco, became the first person arrested for sending SPIM after he flooded MySpace.com with roughly 1.5 million SPIM messages. Anthony literally overwhelmed those users with SPIM ads for mortgage refinancing and inappropriate adult sites. If you're thinking that he couldn't have expected much click through on the mortgage ads, you may have missed the point. Anthony's real goal wasn't to sell the services being SPIMmed; it was to extort money from MySpace. He actually contacted them and offered to protect their users against SPIM for a mere $150 a day. That turned out not to have been his brightest move. Greco was arrested at the Los Angeles airport where he thought he was flying out to meet Tom Anderson, president of MySpace,

to sign a payment agreement for the extorted funds. Some criminals just don't think it through.

SPIM, like SPAM, also often exists to redirect users to malware sites. In May 2009, Facebook users were inundated with messages asking them to "look at mygener.im." Users who clicked on that link were directed to an adware website.

Frequent targets of both SPIM and SPAM, the social networks are beginning to fight back with lawyers as well as security updates. Recently, Facebook was awarded a $711 million judgment against so-called "spam king" Sanford Wallace for his attacks on Facebook users. While Wallace is unlikely to ever pony up that much cash, the civil suit marks a new aggressive stance by social networking sites against spammers.

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

www.100pagepress.com

page press
Smart Books for Smart People®