OWN YOUR SPACE

Compliments of Microsoft

Nasty "ware"

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)

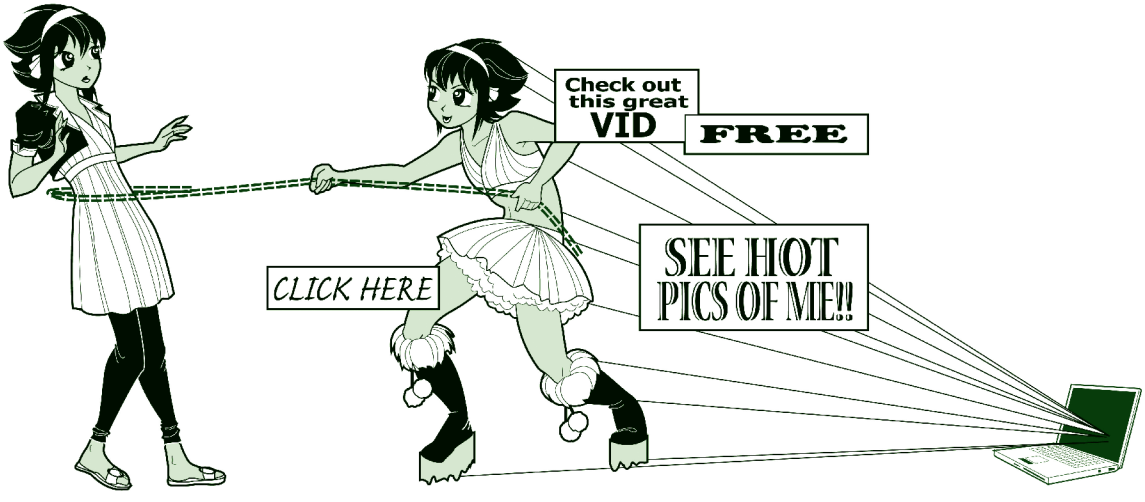
Chapter 3

Nasty "ware"

Meet Stef from Camden, Maine. Stef loves music and enjoys downloading the latest hits to her iPod.

When Stef received an email offering her ten free songs, she didn't hesitate to click the embedded link for more details. Now her PC is under siege from advertisers and continually plagued with pop-up ads.

Stef thought she was only getting a few songs. Little did she know that "free" doesn't always mean "free."



ISBN 978-0-615-37366-9

Stef had fallen victim to adware—one of a number of nasty "ware" problems out there. Like spyware, rogue security software, and ransomware, adware is a major problem for users. While Stef thought her antivirus software would protect her from problems like this, doing that's a lot harder than it sounds. Adware and spyware are really in a class of their own. McAfee refers to programs like these as potentially unwanted programs or **PUPs**. That's a bit generous, since most spyware is unwanted, and we've yet to meet anyone who *really* wanted adware. And while security software like antivirus products try to stop PUPs, or at least warn you about them, the adware writers are continually changing their software to avoid detection.

PUPs Potentially Unwanted Programs. A politically correct term for unwanted adware and spyware.

Still, those PUPs are being dumped on systems and some are collecting data about you. These **data grabbers** often collect information without your knowledge and send that information on to someone else or save it in a special file for pickup later (at the convenience of the hacker). Sometimes, a third party uses the information to target advertising. They're basically looking for better ways to sell you things. Other times, that information is used to steal your identity or take over your computer.

Data grabbers Software programs that collect information about you and send that data on to a third party. Data grabbers include adware, spyware, and keyboard loggers.

3.1 Spyware

Some companies sell legitimate "spyware" programs. Many forms of parental control programs in effect spy on users. So do employee monitoring programs. These are not what we mean when we talk about spyware. In this book, we cover malicious spyware. That is, programs installed without your knowledge that can eat up system resources, affect performance, and steal confidential information. As the name suggests, **spyware** literally spies on you when you use your computer. Among other things, it may keep track of which websites you visit and what you

do on those sites. Spyware may also include keyboard loggers which collect the user names and passwords that you enter at various sites.

Spyware A software program that monitors your computer usage without your knowledge.

Spyware is different from worms and viruses in that spyware's primary purpose is to spy on you. It doesn't self-replicate. Even so, spyware is just as dangerous. If you care about your privacy, you need to understand how spyware lands on your machine and whether you or your parents are at risk.

If your system has slowed down for no apparent reason, you may already have spyware because you visited a malicious or compromised website and the program installed without your knowledge. This type of code dumping is called a **drive-by download**. Some spyware will even install after you say No to installing it.

Drive-by download A program that is installed without your knowledge when you visit a malicious or compromised website.

3.2 Adware

Depending on who you ask, **adware** is either legal commercial software or it's malware that's dumped on a users' systems without their knowledge or truly informed consent. Some people refer to adware and spyware as the same thing, but they're not.

Adware is a type of software that delivers advertising to your Web browser. Advertisers also use adware for what they call behavioral targeting. It allows them to target ads to the consumers most likely to purchase a given product based on those consumers' other online activities. There actually are some legitimate uses for adware, and most adware manufacturers try to stay within the letter of the law by requiring users to consent to having their programs installed.

Adware A program that delivers targeted advertising content to users often by gathering information from a user's computer about what that person does online and which websites are visited.

Adware can be incredibly annoying. It can change your homepage, flood your screen with multiple pop-up ads, install tool bars in your Web browser, and read cookies installed on your computer. It can also arrive without your knowledge.

Teens who are heavy Internet users can easily get adware dumped on their PCs without realizing it. These programs can hitch a ride when you download free tools such as screen savers, or if you visit a malicious website. Teens also often download adware along with popular software, music, and video files.

While adware is usually unwanted, sometimes it's an "I'll scratch your back if you scratch mine," situation. In a common scenario, websites will allow you to download "free" software in exchange for taking adware as part of the package. Of course, that software really isn't free. You're *selling your time* in watching (closing, or trying to close) all the pop-ups in exchange for the software. This may not necessarily be a bad deal. Consider. If your cable company gave you free cable TV in exchange for using a system that stopped you from filtering out the commercials, you might still feel you were getting the better end of the bargain. That's pretty much the deal you're making when you use some popular file-sharing software. The trick is to realize the deal you're making.

3.2.1 End User Licensing Agreements (EULAs)

Many users don't realize that they've consented to install adware because they don't read the **End User Licensing Agreement (EULA)** when they install new software or sign up for new Internet services. This is understandable. EULAs are typically long, boring, and written in legalese. Often, they're presented in small type and confusing language, and most users wrongly assume they don't cover anything that's terribly important. Some companies provide EULAs that are written in such wordy, convoluted text that only the most determined geek will even attempt to decipher their meaning. The adware application TinkoPal provides a EULA that contains over 5,000 words artfully arranged into only 145 sentences of nearly 40 words each.

EULA End User Licensing Agreement. This is the detailed legalese document that you must agree to in order to install most programs.

While it's hard to get around deliberately misleading EULAs, truthfully, few companies bother because they assume you're not going to read the EULA anyway. Quite a few are very upfront and actually list the adware functions. This type of download leaves the adware company on legal ground, because they can argue that you said yes to installing it in the first place, even though you may feel that you were tricked.

3.2.2 Peer to Peer (P2P) Networks

Peer-to-Peer (P2P) networks are places where teens often visit to share resources such as music, films, software, games, and other programs. While it's gone seriously commercial now, Napster began as a popular P2P network. With P2P, you can search online and share files with other people who are using the same file sharing program. Common file-sharing programs include Kaaza, LimeWire, iMesh, and Bit Torrent.

Downloading items from P2P networks is very popular for a number of reasons. These are places to find content that's offbeat, new, or edgy. If you're looking for Indie retro techno-punk, you're probably going to find it on a P2P site. Downloads from P2P sites are also often free. And risky.

Why risky? Commercial sites tend to be extremely careful about what they allow to be downloaded. If they aren't, people are likely to sue them for downloads that trash their systems. Artists are likely to sue them for violating copyright laws. When money's involved, people are likely to sue in general. While those lawsuits (or just the fear of them) drive up the price, they also add incentive to site operators to ensure that their downloads are safe and legal.

Things get riskier when you start downloading from unknown sites and sites that rely on individual submissions such as P2P networks. Downloading games, movies, and music from unknown sites can get you into trouble on several levels. You might download malware, adware, spyware, Trojans, and keyboard loggers. You may also violate copyright laws and face fines for piracy. Even if the material you're downloading is safe, your download experience may be more than you expected. Specifically, you may have agreed to accept adware when you installed the software you need for P2P file sharing.

At this point you're probably thinking, but I really *need* to download free stuff! That's one of the reasons I wanted a PC to begin with. Don't despair. While you may or may not *need* to download free stuff, you certainly don't *need* to use an adware version of download software to do so. Many P2P services offer a commercial download package that's free of adware. The catch of course, is that it is commercial—meaning you'll need to pay for it. If the price tag makes you balk, remember that you ARE paying for the free downloads. You're selling your time (to watch ads) and details on your personal browsing habits. For many people, that price is simply too high.

3.2.3 Downloading Safely

There are many "things" you can download to your computer—a song, a film, a new screensaver, a game, another type of software program. But before you download anything ask yourself these questions:

1. Can the site you're downloading from be trusted?
2. Is the "thing" you're downloading a legal copy or do you think it's probably pirated? Are you breaking copyright laws?
3. Will adware get dumped on your computer? (Not sure? Carefully read the End User License Agreement!)
4. Is the file-sharing software you're using to download this item really free? Or, are you paying for it by selling your time to watch ads? If so, are you OK with that?
5. Is the "thing" you want to download safe? Could it contain malware like a Trojan? Are you willing to take that risk?

3.3 Keyboard Loggers

Keyboard loggers are integral parts of some adware and spyware programs. Other keyboard loggers are installed separately as standalone programs, and marketed as employee or parental monitoring systems.

A **keyboard logger** is exactly what it sounds like, a program that logs every keystroke that you type at your computer. This can be incredibly dangerous. Just think about some of the things that you type in. If you use online banking, you enter the user name and password for your bank account, maybe even the account numbers. If you order games or clothes online, you enter your parents' credit card numbers. If you apply for credit or jobs online, you enter your social security number and other personal data—everything a thief would need to take over your identity.

Keyboard logger A program that keeps track of every keystroke that you type at your computer.

Hackers have been planting keyboard loggers on users' PCs without their knowledge for many years. Short of outlawing keyboard loggers, which probably wouldn't help anyway, the only solution to this problem is to adequately protect your machine. Outlawing loggers isn't an option anyway. Keyboard loggers are a standard part of any security expert's tool bag. Experts use these tools in investigations to catch bad guys doing bad things.

As an interesting side note, some of these keyboard loggers are marketed to parents to monitor teen activity online! If you think you're immune, reconsider. A 2007 study by the Pew Internet & American Life Project found that 53% of parents with home Internet access use monitoring software. In addition, 45% use filtering software to completely block certain sites or types of material. Of course, sometimes it's the teens doing the monitoring. In mid-2008, a high school senior at an affluent California high school was arrested for installing software to track passwords on the school registrar's computer and then using the stolen passwords to change his grades.

3.4 Rogue Software and Scareware

In a cruel twist, some "spyware" exists only to sell anti-spyware solutions. These scams are referred to as **rogue security software** or **scareware**. Rogue software pretends to be legitimate security software. Some of these programs are quite

sophisticated and actually appear to BE your own security software informing you of a problem.

Rogue Security Software Also known as scareware. Applications that use unethical marketing practices to trick users into paying for and downloading worthless or malicious software masquerading as computer security software.

The most common rogue security software displays a bogus message announcing that your computer has been infected with spyware. The message is often formatted to display as if it were coming from your own security software.

The scammer then tries to sell you software to remove the "discovered" spyware. To add an air of legitimacy, most rogue security software uses a name that sounds trustworthy and familiar. The top sellers in 2009 were SpywareGuard 2008, AntiVirus 2009, SpywareSecure, and XP AntiVirus. Often, the same web page that generates the pop-up ad claiming your machine is infected actually *does* infect your computer with malware that continually redirects your web browser to ads for their software. Naïve users find that purchasing that software, for an average $49.95, just installs new and different spyware, and victims generally end up with a computer that's unusable.

This is an old game with a new face. In October 2004, the Federal Trade Commission filed charges against three companies, Seismic Entertainment Productions, Smartbot.Net, and Sanford Wallace, for what amounted to spyware extortion. The three firms first infected PCs with spyware that overwhelmed users with unwanted pop-up ads, then tried to sell them anti-spyware programs to fix the problems they'd just caused.

While the game is old, the tactics are new and evolving. Scareware ads now routinely appear where users don't expect them—like in the top page of search results from major search engines. How? Volume for one thing. By spring 2009, AVG's free LinkScanner tool, which helps prevent users from clicking on malicious Web links, was picking up 30,000 web pages a day that contained ads for scareware.

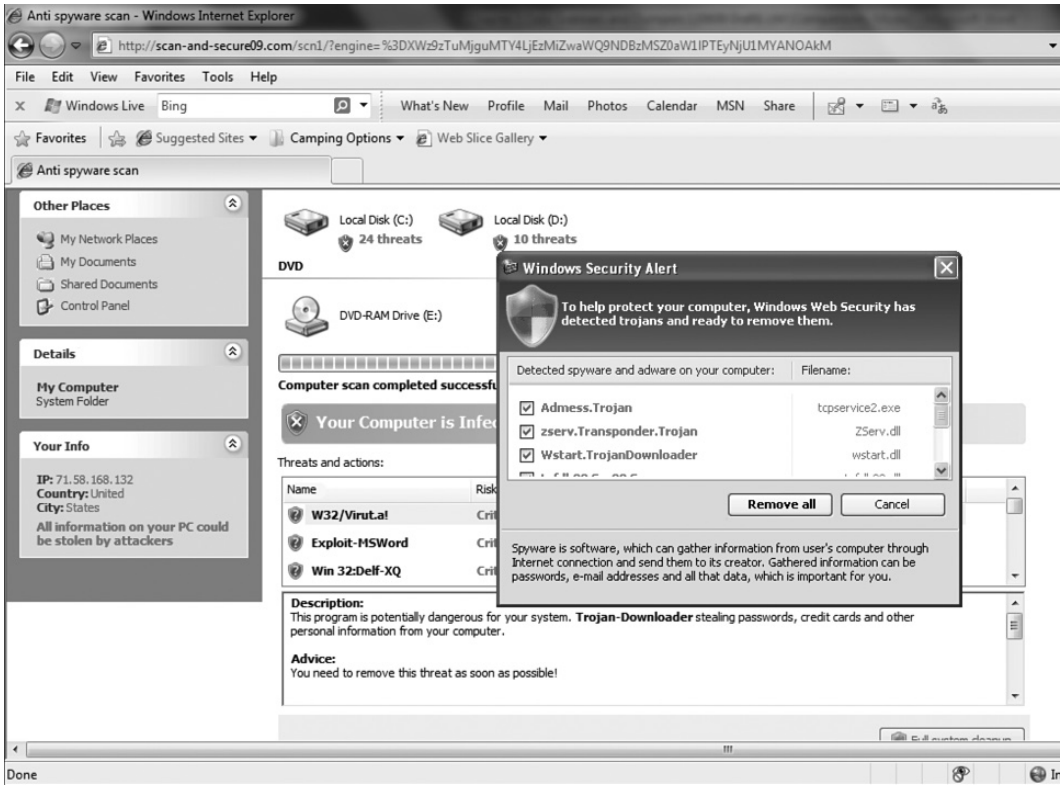
To increase hit rates, the scammers also include phrases that people are likely to search for often, like *American Idol* winner or NASCAR schedule. (We talk about this process, called black hat search engine optimization, later in this chapter.) Scammers also increasingly embed links on social networking sites, Twitter posts, and even within comments made on YouTube videos. In a practice known as **malvertising** (short for malicious advertising), ads for rogue security software have popped up on reputable sites (including Newsweek, Fox News, and the New York Times). The idea is to take advantage of users' trust of the reputable site.

Malvertising The practice of advertising rogue security software on reputable websites to exploit users' trust of those sites.

These scams are extremely common. Here is one we came upon while updating this book. At first glance, it looks legitimate doesn't it?

Our tip-off here was that our computer security software isn't named Personal Security and the people who wrote it understand enough English to write a better warning than "This computer is in danger with malware!" Truthfully, most rogue security software is more professionally written.

At the next level, they did do a better job at the scam. Notice how the next web page displayed looks like it isn't a web page at all unless you look at the address bar at the top. Instead, it's designed to look like a warning message from Windows.



Note that this is complete with the Windows logo on the pop-up identifying the alleged malware.

Regardless of what you click on this screen, you proceed to the download option.

Again, it doesn't much matter what you click here. Most scareware continues the download to infect your computer regardless of what you do at this point—**Run**, **Save**, or **Cancel**. If you're not running a good anti-malware program before you hit this point, you're in serious trouble.

This old game isn't likely to end soon. In April 2009, the *Wall Street Journal* reported that the number of scareware programs had tripled between July and December of 2008. By late 2008, the Anti-Phishing Working Group (APWG) identified over 9,000 separate scareware programs circulating on the Internet. In the first half of 2009, the APWG identified a **583%** increase in scareware programs. The scams appear nearly everywhere, including corrupted emails and even inside comments containing links on legitimate sites like YouTube and Twitter.

3.5 Ransomware

With **ransomware**, the creeps up the ante by holding your computer hostage until a ransom is paid. What distinguishes ransomware from general scareware or rogue security software is that the malware writers disable or threaten to disable your computer unless you pay up. Sometimes, that's an empty threat but one that it's fairly hard for the user to assess.

The most common form of ransomware is an extension of rogue security software. In this scenario, the malware you inadvertently install in response to the bogus spyware or virus report actually disables your files or critical programs until you purchase whatever software it is that they're trying to sell. Sometimes, however, the scammers give up the pretense of selling a product and are just upfront about the extortion.

Ransomware A form of malware in which the user's computer files are encrypted or the system (or Internet connected cell device) is disabled if a ransom isn't paid.

Ransomware is a form of malware that often targets mobile devices. Often, the "ransom" consists of sending a premium ($$$) SMS (text) message. One recent infection, Trj/SMSlock.A, demanded that infected users send a premium text message and include a supposedly unique number in order to receive the deactivation code. Thankfully, the code writers weren't very bright and security experts were able to release a free tool that generated deactivation codes. And by not very bright, we mean really, *really* not very bright, given that they displayed their ransom demands and instructions only По-русски (in Russian).

Most ransomware writers are brighter, albeit just as sleazy. One piece of malware spread in May 2009 through infected links in Twitter posts shut down and disabled all other software applications until victims purchased a two-year license of a rogue security software package for $49.95.

The crooks also don't always lock down your whole machine—just the files you're most likely to use. The LoroBot ransomware, identified in October 2009, encrypted all of the victim's text files, Word documents, PDFs, and JPG picture files, then demanded $100 for the decryption software.

3.6 Black Hat Search Engine Optimization

If you search online often, you know that even the most carefully worded search can return hundreds or thousands of results. While that seems great for all the websites returned, in practice, you know you're not going to look at more than the first few pages of any search result. In fact, odds are pretty high that you won't look at anything after the first 20 sites listed. Companies know this, and put a lot

of work into making sure that their websites appear within those first twenty sites returned. That process of ensuring that a website is returned as high as possible within a search result is called search engine optimization (SEO).

How does this work? The ranking assigned to any search result depends on a lot of factors. While most people assume that the top result is simply the most popular site, that's not the only factor considered. Google claims to use over 200 different factors when ranking websites. Although Google keeps their factors secret to attempt to foil spammers, most of the techniques used by the major search engines are well known. The popularity of a site, the content, the number of sites that have links pointing to it, and other factors are all used in search engine algorithms to determine a site's ranking. SEO uses these known factors to improve a website's ranking.

That ranking is very important. The higher a website is in search engine results, the more people will find the site. Most website operators want their sites listed on the first page of search results—the higher up, the better.

So, how does a website get a higher ranking? Well, content is the primary factor. The better the content, the higher number of links pointing to it. But quality of content is not the only factor. In fact, a website with quality content may not see a lot of new visitors with lower search engine results. No one will find the site. Enter the consultants, specifically, the Search Engine Optimization (SEO) consultants. Optimization is a fancy way of saying that a website will use the search engine algorithms to its advantage to gain a higher search engine ranking. SEO techniques and consultants modify the content and other data on websites and web pages to boost a website's ranking. Most of the major search engine operators even publish information for webmasters on how to structure their websites to do well.

By itself, SEO is a perfectly legitimate business practice. Where it becomes problematic is when it's used in sleazy ways. Have you ever done a search and gotten results that had NOTHING to do with what you searched for? Have you noticed returns for what looks like rogue security software when you searched for something completely unrelated to security? Well, some SEO techniques manipulate search engine algorithms using deception and illegitimate and unapproved means. These techniques are called **black hat SEO**. Some of the deceptive techniques include

stealing legitimate content from a popular website and posting it on a SPAM site, offering legitimate looking content to the search engine for ranking but providing SPAM sites to normal web surfers, and filling a web page with repeated words to increase the keyword counts for the search engine. The major search engines don't approve of these techniques and have modified their algorithms to lower the ranking on websites that attempt these techniques. That is, when they find them.

Black hat SEO The practice of using deception to give a website a higher search engine ranking than it deserves. Often used to direct unsuspecting searchers to pages filled with malware (like rogue security software).

Besides SPAM, black hat SEO techniques have been used for even more dangerous purposes. The main reason that SEO techniques are used is to increase the number of web browsers visiting a specific site. If a hacker wants you to try out his latest piece of malicious software, what better way to get interest in it? If he creates a website and uses black hat SEO techniques to get more people to find it, he'll have a large number of people to test it out for him. For the hacker, little effort is really needed to raise search engine rankings for his site.

Depending on his choice of keywords, the hacker can even pick a specific group of people to target. Kids are more likely to search for keywords like "algebra homework help" or "jonas brothers" than "retirement" or "dentures." Using black hat SEO allows a scam artist to route a teen searching for a particular gaming site to a fake gaming site that actually downloads malware instead of games. Always be careful when looking through search results. Just because a site is returned at the top of the list doesn't mean the site is necessarily relevant or safe. If the search engines can be fooled, so can you.

3.7 Current and Future Threats

The battle between users and hackers is a classic arms race. Both sides strive to stay one step ahead of the other. Recently, that struggle has become much more complicated for users. In the past, we only needed to worry about our home computers, and we could usually protect those fairly well with a standard antivirus software package.

Times have changed. Today's users spend more time online and on the go. Our computers now fit in our pockets and connect us with everyone, everywhere, at any time. We connect with our peers not just through email, but with tweets, texting, and real-time updates on Facebook and MySpace.

We expect—and get—instantaneous communication. Standing in line at a movie? We pull up reviews on our iPhones, check for tweets from friends who watched the film earlier.

While we're reaching out to the world, hackers take advantage of our connectedness and our willingness to trust. They find vulnerabilities in our smart phones, trick us into installing malware, corrupt search engine results, put up fake websites that look like the real thing, and use our constantly connected computers in botnets that deliver SPAM, attack other computers, and attempt to alter search results.

And the arms race continues. Hackers are constantly challenged to find new vulnerabilities, bypass security software, and trick users. Users must be constantly vigilant by installing and updating legitimate security software, updating that software as vulnerabilities are discovered, and avoiding the minefield of phishing scams, rogue software attacks, and fraudulent websites that deposit malware.

What does the future hold? For hackers, obviously more of the same. Hackers will continue to exploit any weakness they can find to get access to our personal computers, our private accounts, and our personal information. It is also likely that they will spread their efforts more widely, and we'll see more attacks on mobile devices. In many ways, our mobile devices are a more inviting target. They contain more personal information, are always connected, and have fewer methods for protection from attack. For users, the future holds greater responsibility and education. Understanding the importance of information security, particularly the security of personal information, will become paramount. And savvy users, like you, will make it a point to learn how and why to protect their data from hackers.

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®