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-Sivy
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

Except where otherwise noted, content in this publication is licensed under the Creative Commons Attribution-Noncommercial-No Derivative Works 3.0 United States License, available at http://creativecommons.org/licenses/by-sa/3.0/us/legalcode.

Library of Congress Cataloging-in-publication Data

McCarthy, Linda
Own your space : keep yourself and your stuff safe online / Linda McCarthy.

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)
It was Friday evening, prime time for playing rounds of online games with friends from school. Douglas, a 15-year-old boy from Novato, California, had—as usual—gone straight from the dinner table to the Net.

Douglas is a serious gamer. He has every game system on the market. He even has two Microsoft Xbox 360s, a Sony Playstation 3, and a Nintendo Wii in his bedroom. Needless to say, he also spends time playing his favorite game, *World of Warcraft*, on the Internet. In the middle of the game, he lost his connection and was dropped from the gaming site. The following message flashed across his computer screen.

Connection Lost Out of Bandwidth!!!

Douglas was annoyed that he couldn’t finish his game and had no clue what that message meant. He started to wonder if he’d been dropped off because of the firewall on his parents’ network. Douglas turned off the firewall, entered the gaming site and began to play his favorite game again. No drop off this time. Douglas decided to leave the firewall off while he was playing his game on the Internet.
While turning off the firewall sounded like a good idea to Douglas, that wasn’t the problem. In fact, that created a new problem because turning off the firewall opened the door to his parents’ home network to hackers. The bandwidth problem had to do with the network in Douglas’s house. He really didn’t have enough bandwidth coming into his house in the first place. In this chapter, you will see how you can test your bandwidth for free. Also, this chapter talks about some of the basics of networking and why firewalls are a critical component of security.

13.1 So What’s a Network?

A computer network is a group of computers that are connected. Sometimes this is a physical connection using wires, cables, telephone lines or some combination of the three. Sometimes, as with “hot spots” and wireless networks, there is no physical connection. In all cases, however, the computers within a network are connected in a way that allows their users to share resources like files and/or physical devices like printers.

At school, the school’s network is what allows you to create your research papers in one computer lab but pick up your printout in another. This is also what allows your teacher to enter grades at the computer on her desk and pick up printouts of student progress reports in the teacher’s lounge.

Computer networks have been around for a long time, and several technologies have been developed to enable computers to communicate. One of the most successful is a technology called Ethernet, invented by Bob Metcalfe in 1973.

**Ethernet** Ethernet lets computers on a Local Area Network (LAN), such as in an office building, connect to one another and to other network resources, such as servers.

Today’s computer networks come in many shapes and sizes. They can be HUGE. A major university might have a computer network that connects thousands of students, faculty, and staff. A computer network can also be quite small. Consider the network at Douglas’s house. That network connects just three computers—one for Douglas, one for his mom, and one for his dad. Because they’re using network technology, the whole family can use the same Internet connection and send files to the same printer.
Regardless of their size, all networks work pretty much the same way and provide the same functions. That is, they all use one **protocol** or another to allow the computers and other devices in the network to talk to each other, and they all provide shared access to network resources. It’s also possible for some resources in a network to be shared by some users but not others. This is why *you* can’t send files to that printer in the teacher’s lounge.

**Protocol**  A protocol is a set of rules that computers use to communicate with each other.

One network can include all or part of another network. For example, the computer in your mom’s home office is obviously part of your home network. However, it might also be connected to your mom’s work network. It’s also part of a network that includes all the machines that use the same **Internet Service Provider** (ISP). And, all of those machines are also part of the massive World Wide Web. So, we have networks inside networks inside other networks.

**ISP**  Internet Service Provider. This is the company that provides the network that allows your computer to connect to the Internet.
13.2 How Networks Communicate—TCP/IP

Being part of a network is like being part of a community. In a community, life runs smoothly only when the people who form the community talk to each other. To share community resources, the members of the community need to communicate in ways that everyone can understand.

Computer networks are much the same. For computers to share resources, they need to communicate using a common language. In computer terms, that common language is called a protocol. A protocol is just a set of rules that computers use to communicate with each other.

TCP/IP is the protocol used most often to communicate on the Internet. TCP stands for transmission control protocol. When you “transmit” something, you are sending it somewhere. Thus, a “transmission” is whatever it is you are sending. So, TCP is the protocol that controls how things are transmitted on the Internet. In specifics, TCP works by sending data in blocks called packets. (When data is sent over the Internet, it is divided up into blocks of data called packets.) IP stands for Internet protocol and describes how computers send those data packets from one computer to another.

TCP/IP The protocol that most computers use to communicate on the Internet.

13.2.1 IP Addresses

For data packets to travel safely from one computer to another, the control protocol needs to know where the packets are going. It needs an IP address to send the packets to. It also needs to know the address the packets are coming from so that it can send a reply back to let the sender know that everything arrived safely.

Just like your house has a mailing address, every computer on the Internet has an IP address. Each IP address contains four groups of numbers separated by periods. For example, 192.168.1.1 is an IP address. Depending on what kind of Internet connection you have and how your ISP assigns addresses, you may have a static IP address or a dynamic IP address.
A static IP address is always exactly the same. Like your house address. That address is assigned when the house is built and it stays the same as long as the house is there. While your house address is assigned by the post office, your computer’s IP address is assigned by your ISP, or possibly by indirectly connected machines if you have a private home network.

The advantage of having a static address for your house is that once a person learns your address, that person will always know your address. With IP addresses, this is a disadvantage. Once a hacker learns a static IP address, he would always know how to get back to that specific computer.

A dynamic IP address is issued when you connect to the Internet on any given day and you keep that address only until you log off the Internet or shut down your computer. The next time you connect to the Internet, you get a new (and probably different) IP address. Dynamic IP addresses help to protect you from being targeted repeatedly by a hacker trying to break into your computer. Your ISP assigns dynamic addresses from a pool of addresses available to that ISP. The protocol that manages the assignment of IP addresses is called **DHCP** (dynamic host configuration protocol).

**DHCP** Dynamic host configuration protocol. DHCP is the protocol that an ISP uses to assign dynamic IP addresses.

Whether you have a static IP address or a dynamic IP address depends on two things: (1) what type of Internet connection you have, and (2) the policies of your ISP.

If your connection is always on, and you have a static IP address, attackers have a better chance of being successful at attacking you. It’s simple to see that if you always have the same IP address you are easier to find. That does not mean that dynamic IP addresses are safe, however.

To find your IP address, first make sure that your computer is connected to the Internet. Now, click **Start > All Programs > Accessories > Command Prompt**. This will open a command prompt window.
Enter the `ipconfig` command at end of the `C:>` prompt line. The window that displays next lists your IP address.
Now, shut down your computer and router and restart both of them. Connect to the Internet again and issue the `ipconfig` command a second time. If the address it returns matches the address it gave you the first time, you have a static IP address. If the two addresses don’t match, you have a dynamic IP address.

You can also find the IP addresses for other computer systems by using the `ping` command. For example, to find the IP address for Google, click on **Start > All Programs > Accessories > Command Prompt** to again open a command prompt window. Then, enter the command `ping www.Google.com`.

The dialog box that displays next shows the IP address for www.Google.com under **Reply from**.

![Command Prompt window](image)

As we just pointed out, an IP address is similar to your home address. Once you have an address to a house, you can knock on the door and you might get in. When you find the IP address to a computer system, you’ve basically found the front door. To protect the front door to your network, you need several layers of defense including a firewall.

### 13.2.2 Data Packets

TCP/IP works by splitting messages and files being sent over the Internet into chunks called packets. Each packet contains part of the message or file plus the address of its destination.
In this type of communication, the computers sending data back and forth are called hosts. The computer sending the packet is the source host. The computer receiving the packet is the destination host. Both hosts use the same protocol to make sure that the packets arrive safely and in the right order.

Imagine that you were sending a book that you’d written from your computer to your teacher’s computer. When you send the file containing the book, the controlling protocol would first split the book into smaller sections (packets). While actual data packets are considerably smaller, to make this simple let’s imagine that each chapter becomes a packet. If there are six chapters in your book, there would be six data packets. Each packet would contain a separate chapter plus the IP address of your teacher’s computer.

The control protocol would also add sequence information (say, the chapter number) to make sure that when the packets are assembled back into a single file at your teacher’s computer, the chapters are still in the correct order. This makes sure that Chapter 1 comes first, Chapter 2 second, etc. To make things even more reliable, the control protocol on your teacher’s computer would send a confirmation back to your computer, letting it know that the packets arrived safely.

13.2.3 Confirmation
There are actually a number of protocols that computers could use to communicate. TCP/IP is simply the most common. Some communications use a different protocol called UDP instead. Most Internet connections, however, use TCP/IP because it’s considered to be more reliable.

TCP is considered more reliable because with TCP the computer sending the data receives confirmation that the data was actually received. UDP doesn’t send confirmations. This makes UDP faster than TCP but not quite as reliable. In some cases, that’s OK. Knowing that something actually made it to the destination is important for some programs, and not for others.

13.3 Port of Call
Where an IP address identifies the general location of your computer, the specific locations through which data actually gets into your computer are called ports. You can think of a port as a door into your computer. Unlike your house, which
probably has only two or three external doors, your computer has 65,535 ports. Some of these ports are allocated to specific applications. For example, AOL Instant Messenger uses port 5190. HTTP, the protocol used to communicate on web pages, runs on port 80 and port 8080.

When we say that an application runs on a specific port, what we really mean is that the application uses a service program to monitor that port. Thus, IM runs a service that hangs out at port 5190. It listens at that port for communications to arrive and responds when it detects those communications. You can think of these services as doormen. They wait at the door to see who knocks. When someone does knock (that is, data arrives at that port), the doormen (services) follow the rules (protocol) they’ve been given to decide whether or not to let the knockers in.

Attackers routinely scan the Internet looking for computers with open (unprotected) ports. This is called port knocking. To protect your computer and its data, you need to make sure that your ports are protected.

**Port knocking** Scanning the Internet looking for computers with open ports.

As you learned earlier, some applications run on specific ports. Of course, there are 65,535 available ports. You can specify access for services on specific ports through your firewall. Your firewall functions as a bouncer at an exclusive club—it has a “guest list” of exactly who is allowed in at which port. Thus, firewalls block access to ports that are not being used for specific applications. A firewall that is configured correctly won’t accept connections to ports unless it’s specifically told to do so. To protect your computer and its data, you need to make sure that your ports are protected. The list of ports and services is too extensive to cover here. You should visit your firewall vendor’s site to see what ports and services are recommended and which ones are considered risky. Another good place to learn about ports and services is www.grc.com.

While you’re still learning about firewalls, a simple step that you can take to protect your computer is to simply turn off your computer and router when you’re not using them. Think about it. Hackers know that many home users leave their systems turned on and connected to the Internet for convenience. Therefore, it makes sense to turn off your computer and router when you are not connected to the Internet.
13.4 A Bit More about Bandwidth

Bandwidth is the speed at which data is sent over a communication line. Bandwidth measures how quickly your PC communicates with the Internet. Our gamer Douglas was dropped from the game he was playing over the Internet when the message *You are out of bandwidth* flashed across the screen. Like most users, Douglas never wondered how much bandwidth he had until he ran out. Do you know how much bandwidth you have?

After Douglas ran into the bandwidth error, his mom checked her cable bill and the website for her cable Internet service. She was paying for a bandwidth of 3 megabits per second. But when she checked the actual bandwidth she was getting, it turned out that only 1.7 megabits was available. She was paying for more than she was getting. When she complained to her ISP, they immediately coughed up the extra bandwidth.

If you’re worried about a similar problem, there are a number of places on the Internet where you can run a bandwidth test on your system for free. One safe site is www.bandwidthplace.com.

Your potential bandwidth will depend on the type of Internet connection that you have.

13.5 Rings of Fire

When you started reading this book, you probably had no idea you had 65,535 available ports on your computer. Watching and blocking all those doors to your computer is one of the most important security jobs you need to fill. We’ve already
talked about a number of products and techniques you can use to protect your computer. A firewall is *one more* important layer of defense.

While you absolutely NEED a firewall, it is only *one* piece of the security protection puzzle. Using a firewall does NOT eliminate your need for other security products such as antivirus and anti-spyware programs unless your firewall comes as part of a bundled security solution. (Some security products aim to provide a total or near-total “solution” to security problems by bundling a whole bunch of different types of protective software into a single product.)

**Firewalls do protect against hackers**

An “intrusion” occurs when an attacker takes over your computer system. Many different techniques are used to hijack systems this way. Hackers might break into your system to leisurely poke around your files and read personal data; they might use your resources, launch a denial of service (DoS) attack, or steal your personal or financial information. Firewalls can help to protect you against many of these attacks by keeping you aware of when an outside program tries to access your computer through its ports or a when program running on your computer tries to access the Internet.

**Firewalls do enforce security policies**

Firewalls also enforce security policies to provide protection from inside out. The library has a firewall. Your school has a firewall. Even corporations have firewalls. In each case, the firewall has probably been set to block access to certain sites. Your school doesn’t want you to visit sites with inappropriate or obscene material that your parents might object to. Your library has probably blocked access to free email accounts. Many libraries do this so that the computers intended to allow patrons to complete Internet research aren’t always filled with people checking their email.

In all these cases, the firewall’s actions represent a policy that was established for a reason. If you’re behind a firewall and decide to try to figure out “a way around
it,” you know that you really shouldn’t be doing that. What you might not know is that what you are doing might be logged by the firewall.

**Firewalls don’t make you behave**

You already know that just because a babysitter comes over doesn’t mean kids will behave. They may not jump out the windows, but that’s not to say they won’t play *Guitar Hero* ’til the wee morning hours. Like a babysitter, a firewall only has so much control. A good firewall will enforce the security policies it’s been set to enforce. Usually, that means that it might block certain sites or prevent certain programs from accessing the Internet. What it won’t and can’t do is make YOU behave online. Your firewall has no say over what you type when IMing your friends, which sites you visit (unless they’re specifically blocked), or what kinds of email you send. Those things, along with the rest of your online behavior, are the products of your choices, not your firewall.

**Firewalls don’t protect against embedded attacks**

Firewalls also don’t protect you against “data-driven attacks.” These types of attacks are initiated by an attack tool or malware that you inadvertently download or receive as an unwanted email attachment. When these attacks come in the form of malware that’s downloaded without your knowledge or permission, they are sometimes called drive-by downloads. For more details on avoiding drive-by downloads, please read *Chapter 3, Nasty “ware.”*

### 13.5.1 So What’s a Firewall?

A **firewall** is a piece of software that protects your computer (or your entire home network) by controlling the type of traffic that’s allowed to pass between networks. In many ways, your firewall is like the lock on the front door to your house. Your front door lock keeps thieves, potential attackers, and nosy neighbors out of your house. By monitoring traffic to and from your computer and watching programs that communicate with your computer, your firewall performs much the same functions. It functions as the lock on your computer’s front door to the
Internet, either permitting or denying program requests to send data into or out of your computer or network.

**Firewall** A piece of software that controls the type of traffic that is allowed to pass between networks.

Amazingly, many people don’t know whether they’re using a firewall. Some users actually have a firewall and don’t even know it. If your home computer is networked, you may already have a firewall included in your router. A **router** is the physical device that routes information between devices within a network.

The major function of a firewall is to control traffic coming from or going to the Internet. Let’s go back to Douglas’s house. On his network, a Comcast cable modem is connected to a Linksys router. The family computers then connect to the Internet through that Linksys router. From the Internet, the only device that can be seen is the router. The family computers are “hiding behind” that router. The router passes along (i.e. “routes”) all information going to and from the Internet. In no way can information get to or from any computer in Douglas’s house without passing through the router.

Because a router protects the machines it routes data to, the router functions like a grand entrance way. That makes it a logical position for a firewall.

**Router** The physical device that routes information between devices within a network.

Of course, the router is not the ONLY place you’ll want a firewall. You should also have a “personal” firewall on the PC itself. The personal firewall will allow you to monitor the applications running on your computer and restrict when and if those programs are allowed to send data to or from your computer. Using a personal firewall also provides a second layer of protection just in case a hacker compromises the firewall on your router. With only the router firewall, a hacker who compromises the router firewall can easily access any computers connected to that router. Add a personal firewall and that hacker has only made his way through your first line of defense.
13.5.2 Network Address Translation

For your first layer of defense, you need to have a firewall at the point where the Internet connects to your computer—that connection point is at your router. Another feature that is important is Network Address Translation (NAT). NAT allows you to use different IP addresses externally than you use internally. This helps to conceal your internal network, letting your home computer(s) “hide” behind your router. We talked earlier in this chapter about how your ISP assigns you an external IP address. A **NAT router** takes that assigned IP address and then distributes its own internal IP addresses to the computers inside your home network. From the Internet, only the router’s address is visible. Because the NAT router assigns its own internal IP addresses, the IP address of each computer remains private.

**NAT router** A router that uses Network Address Translation to keep the IP address of your computer private and unviewable from the Internet.

Like operating systems and major application programs, routers also have known security holes. Therefore, you’ll want to apply any patches or updates as needed. For most routers, you will also need to change the default login and password and make sure that the firmware is current.

13.5.3 So How Do Firewalls Protect Me?

Firewalls have two major protective functions:

- They permit or deny requests to send data to or from your computer.
- They monitor port access requests.

**Permitting or Denying Data**

There are two strategies you can choose from when setting up your firewall: a default permit strategy, or a default deny strategy.

- A **default permit** strategy means you configure the firewall to allow any host or protocol that you haven’t specifically banned.
A default deny strategy means that you list specific protocols and hosts that are allowed to pass through your firewall. Everything else is denied.

You’ll notice that there’s a world of difference between these two approaches. While default deny is a more censored and potentially robust approach, it’s also a lot harder to configure. Unless you put a lot of work into your definitions, a default deny strategy could become so restrictive that your Internet connection might lose its utility. Default permit, of course, is much easier to configure—you basically block out known dangers, adding new blocks as new dangers are discovered. With default permit, you’re allowing anything in until it’s proven dangerous. With default deny, you’re denying everything until it’s proven safe.

**Monitoring Port Access Requests**

Firewalls monitor and regulate connections in and out of your computer by looking at everything that tries to access a port. You can configure your firewall to alert you every time an application or protocol tries to access a port.

Of course, ports that let data out can also let data in. Attackers often try to gain access to computer systems by first scanning for open ports. To protect your machine from port knocking, you need to configure your firewall to monitor and possibly block inbound connections. Attackers know that home users often don’t install firewalls and frequently leave ports wide open—even ports on which vulnerable services are running. If you want to learn more about ports, services, and how firewalls work, a good place on the Internet is Steve Gibson’s site, www.grc.com.

**13.5.4 Firewall Settings**

Techies can dig down into the heart of a firewall and block specific ports or applications. Most other users really prefer not to. Thankfully, most firewalls give you the flexibility to install quickly and easily by simply configuring your firewall setting to high, medium, or low. Which setting is best for you depends on what you do on the Internet.

We strongly suggest that you start by setting your firewall to High security. If you need to, you can adjust the level down from there to Medium. (“Low” security is rarely a wise idea.)
While you’re setting up your firewall, don’t forget about the logs. Firewall logs keep track of who and what tries to communicate with your system. It’s nice to know who’s poking around (or trying to peek) at your machine!

13.5.5 Free Firewalls
In recent years, firewalls have become more powerful, much more important, and—equally important to many users—fairly cheap. Better than cheap, some firewalls are actually free. You can get the free firewall Zone Alarm from www.zonelabs.com.

One frequently used firewall to beware of is the one built into Windows XP. That firewall only blocks inbound connections; it does nothing to block outgoing connections. Windows Vista and Windows 7 firewalls both fix that shortfall and block both inbound and outbound connections. To understand your firewall protection, make sure you know which OS your PC is running.
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.