Home Computer Security

FedCIRC

This work was produced for FedCIRC and the General Services Administration by the CERT® Coordination Center, Software Engineering Institute, Carnegie Mellon University.

Contents

Introduction 1

Thinking About Securing Your Home Computer.....3

Things You Ought To Know 4

What Should I Do To Secure My Home Computer? 7

Summary.....33

End Notes 34

Acknowledgements 34

Property has its duties
as well as its rights.

Thomas Drummond (1797-1840)

Home Computer Security

Introduction

Your home computer is a popular target for intruders. Why? Because intruders want what you've stored there. They look for credit card numbers, bank account information, and anything else they can find. By stealing that information, intruders can use your money to buy themselves goods and services.

But it's not just money-related information they're after. Intruders also want your computer's resources, meaning your hard disk space, your fast processor, and your Internet connection. They use these resources to attack other computers on the Internet. In fact, the more computers an intruder uses, the harder it is for law enforcement to figure out where the attack is really coming from. If intruders can't be found, they can't be stopped, and they can't be prosecuted.

Why are intruders paying attention to home computers? Home computers are typically not very secure and are easy to break into. When combined with high-speed Internet connections that are always turned on, intruders can quickly find and then attack home computers. While intruders also attack home computers connected to the Internet through dial-in connections, high-speed connections (cable modems and DSL modems) are a favorite target.

No matter how a home computer is connected to the Internet, intruders' attacks are often successful. Many home computer owners don't realize that they need to pay attention to computer security. In the same way that you are responsible for having insurance when you

drive a car, you need to also be responsible for your home computer's security. This pamphlet explains how some parts of the Internet work and then describes tasks you can do to improve the security of your home computer system. The goal is to keep intruders and their programs off your computer.

How do intruders break into your computer? In some cases, they send you email with a virus. Reading that email activates the virus, creating an opening that intruders use to enter or access your computer. In other cases, they take advantage of a flaw or weakness in one of your computer's programs – a vulnerability – to gain access.

Once they're on your computer, they often install new programs that let them continue to use your computer – even after you plug the holes they used to get onto your computer in the first place. These "backdoors" are usually cleverly disguised so that they blend in with the other programs running on your computer.

The next section of this pamphlet discusses concepts you need to know, especially trust. The main part of the pamphlet explains the specific issues that need your attention. Most sections conclude with a reference to a web site that you can use to find examples of how to do some of these tasks to secure a Microsoft Windows 2000-based computer. Near the end of the pamphlet, there is a reference to a web site that contains checklists you can use to record information about the steps you have taken to secure your computer.

Whether your computer runs Microsoft® Windows®, Apple's Mac OS, LINUX, or something else, the issues are the same and will remain so as new versions of your system are released. The key is to understand the security-related problems that you need to think about and solve.

Thinking About Securing Your Home Computer

Before diving into the tasks you need to do to secure your home computer, let's first think about the problem by relating it to something you already know how to do. In this way, you can apply your experience to this new area.

So, think of your computer as you would your house, your apartment, or your condo. What do you know about how that living space works, what do you routinely do to keep it secure, and what have you installed to improve its security? (We'll use this "computer-is-like-a-house-and-the-things-in-it" analogy throughout, departing only a few times to make a point.)

For example, you know that if you have a loud conversation, folks outside your space can probably hear you. You also routinely lock the doors and close the windows when you leave, and you don't give the keys to just anyone. Some of you may install a security system to complement your practices. All of these are part of living in your home.

Let's now apply similar thinking to your home computer. Email, instant messaging, and most web traffic go across the Internet in the clear; that is, anyone who can capture that information can read it. These are things you ought to know. You should always select and use strong passwords and exercise due care when reading all email, especially the unsolicited variety. These are things you ought to do. Finally, you can add a firewall, an anti-virus program, patches, and file encryption to improve the level of security on your home computer, and we'll call these things you ought to install.

The rest of this pamphlet describes the things you ought to know, do, and install to improve the security of your home computer.

Things You Ought To Know

One starting point for solving home computer security problems is being aware of how the Internet and some of its technologies work. If you know how they work, you can evaluate solutions to the problems that come up. You can also use the Internet more safely and responsibly. In this section, we'll talk about two topics: trust and information in the clear as it crosses the Internet.

Trust

Human beings are trusting by nature. We trust much of what we hear on the radio, see on television, and read in the newspaper. We trust the labels on packages. We trust the mail we receive. We trust our parents, our partner or spouse, and our children. We trust our co-workers. In fact, those who don't trust much are thought to be cynical. Their opinions may be all too quickly ignored or dismissed.

The Internet was built on trust.[1] Back in the mid 1960s, computers were very expensive and slow by today's standards, but still quite useful. To share the expensive and scarce computers installed around the country, the U.S. government funded a research project to connect these computers together so that other researchers could use them remotely. This project was called the ARPAnet, named after the government research agency – ARPA, the Advanced Research Projects Agency – that funded and managed the project.

Key to the ARPAnet was the level of trust placed in its users; there was little thought given to malicious activity. Computers communicated using a straightforward scheme that relied on everybody playing by the rules. The idea was to make sharing

ideas and resources easy and as efficient as the technology of the day provided. This philosophy of trust colors many of the practices, procedures, and technologies that are still in place today.

Only within the last few years, when Internet commerce (known as e-commerce) began to spread, it has become inadequate to rely principally on trust. Since the days of the ARPAnet, we've changed the way we use computer networks while others have changed the underlying technologies, all in an attempt to improve the security of the Internet and the trust we place on it.

Let's dig deeper into two examples of what we trust in our daily lives. When you receive mail through the post office, many envelopes and the letters in them contain the sender's address. Have you ever wondered if those addresses were valid; that is, do they match the address of the person or persons who really sent them? While you could check to see that those addresses are valid and refer to the person they name, it's not an easy task.

How would you go about it? Would you call the phone number provided with the letter? That number could also be invalid, and the person that answers the phone could be as misleading as the original address. Perhaps you could call directory assistance or the police department that has jurisdiction over the town where the letter was supposedly from. They might be helpful, but that is likely to take lots of time. Most people wouldn't bother.

And it's not just return addresses either. How about advertisements, news stories, or the information printed on groceries? Suppose you were on a low-fat diet. You'd want to buy foods low in fat. To select the right foods, you'd read the product label at the grocery store. How do you know that the label information is valid? What's to say it's not forged? And how would you know?

The Internet has many of the same issues, and email is one of the best examples. In an email message, an intruder can easily fabricate where the came from. But this information forging – called spoofing by intruders and security professionals – is not limited to just email. In fact, the basic unit of information transferred on the Internet – called a packet – can also be easily forged or spoofed.

What does this mean and why should you care? It means that any information you receive from some other computer on the Internet should not be trusted automatically and unconditionally. When you trust an email message that turns out to have a harmful virus attached

to it, your computer can be infected, your files destroyed, and your work lost. And that's why you should care.

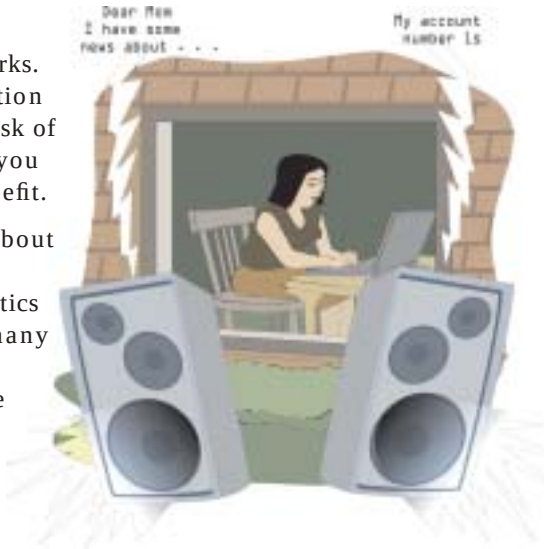
This is how the Internet works. It was built on trust. Over time, there have been technological changes that are worthy of a higher level of our trust than before. Nonetheless, a true sense of insecurity is better than a false sense of security. So, think about the information you trust. Be critical and cautious.

Information in the Clear

When you have a conversation with someone in your living space, everybody within earshot can hear the words and probably understand them. If your conversation is especially loud and your windows open, even passersby can hear. If you want privacy, you and your conversation partner need to go to another room and close the doors and windows.

The Internet works much the same way, except the room is much, much bigger. When you send email, browse a web site, or chat online with someone, the conversation between you and that person does not go directly from your computer to his or her computer. Instead, it goes from your computer to another computer to still another computer and so on, eventually reaching his or her computer. Think of all of these computers as an Internet "room."

Anyone, or, more accurately, any program, in that Internet room that can hear that conversation can also probably understand it. Why? Because just like the conversation at home, most Internet conversations are in the clear, meaning that the information exchanged between computer systems is not concealed or hidden in any way.



Again, this is how the Internet works. You need to know that the information sent across the Internet may be at risk of others listening in, capturing what you send, and using it for their own benefit.

Later in this pamphlet, we'll talk about encryption as a way to address this problem. Encryption uses mathematics to conceal information. There are many programs you can install to encrypt the information you send across the Internet.

What Should I Do To Secure My Home Computer?

Securing your home computer is not a trivial task. There are many topics to consider and many steps to follow. They take time to learn and do. If you can, read this entire pamphlet before you begin to secure your computer. You'll have a better understanding of the effort and all its facets. This ought to help you when you begin to tackle the tasks described here.

In the following sections we describe two types of activities. Some you can do using the programs that came with your computer: working with passwords and email attachments, running programs, and backing up your work. For other activities, you might need to obtain some specialized programs: applying patches, and running anti-virus, firewall, and file encryption programs. Though some vendors' products provide these features, we'll assume your computer doesn't have any of them so you'll need to add all of them.

Here then is the list of tasks you need to do to secure your home computer. Their order is based on how intruders attack computers, beginning with the most-often used attack methods. By starting with the lower numbered tasks, you address the biggest problems you face in securing your home computer. Remember that most sections end with a reference to a web site that you can use to find an example of how to do the task on a Microsoft Windows 2000 computer.

Task 1 - Install and Use Anti-Virus Programs

If someone rang your doorbell and wanted to come into your living space to sell you something or to use your telephone, you'd need to make a decision whether or not to let them in. If they were a neighbor or someone you knew, you'd probably let them in. If you didn't know them but believed their story and found them to be otherwise acceptable, say they were neat and clean and not threatening, you'd probably also let them in, but you'd watch them closely while they were in your space.

What are you doing here? You are profiling this person and then deciding what to do based on that profile. It's your responsibility to be concerned about who enters your living space. Further, if you have

children, you've probably also taught them how to deal with strangers who come to your door.

Anti-virus programs work much the same way. These programs look at the contents of each file, searching for specific patterns that match a profile – called a virus signature – of something known to be harmful. For each file that matches a signature, the anti-virus program typically provides several options on how to respond, such as removing the offending patterns or destroying the file.

To understand how anti-virus programs work, think about scam artists – people who visit your home to try to get you to buy a phony product or service, or to let them in. Once inside, they may try to steal your valuables or try to harm you in some way.

There are a variety of ways you might find out about a specific scam artist lurking in your neighborhood. Perhaps you see a television report or read a newspaper article about them. They might include pictures and excerpts of the story the scam artist uses to scam their victims. The news report gives you a profile of someone you need to be on the lookout for. You watch for that person until either the story fades away or you hear that they've been caught.

Anti-virus programs work much the same way. When the anti-virus program vendors learn about a new virus, they provide an updated set of virus signatures that include that new one. Through features provided by the updated anti-virus program, your home computer also automatically learns of this new virus and begins checking each file for it, along with checking for all the older viruses. However, unlike scam artists, viruses never completely fade away. Their signatures remain part of the master version of all virus signatures.

Suppose a scam artist was at your front door. What would you do? Perhaps you'd not encourage them to come in nor buy their product but, at the same time, you'd try not to upset them. You'd politely listen to their story and then send them on their way. After you closed the door, you may call the police or the telephone number given in the report that initially brought them to your attention.

With viruses, you often have the chance to react to them when they've been discovered on your home computer. Depending upon the specific characteristics of the virus, you might be able to clean the infected file. Or you might be forced to destroy the file and load a new copy from your backups or original distribution media. Your options depend upon your choice of anti-virus program and the virus that's been detected.

In your living space, you look at those who come to your door and you look at what you receive in the mail. These are two of the ways that items can get into your living space, so you examine them, sometimes closely, sometimes not.

Viruses can reach your computer in many ways, through floppy disks, CD-ROMs, email, web sites, and downloaded files. All need to be checked for viruses each time you use them. In other words, when you insert a floppy disk into the drive, check it for viruses. When you receive email, check it for viruses (remember to use the **KRESV** tests described in Task 3, *Use Care When Reading Email with Attachments*). When you download a file from the Internet, check it for viruses before using it. Your anti-virus program may let you specify all of these as places to check for viruses each time you operate on them. Your anti-virus program may also do this automatically. All you need to do is to open or run the file to cause it to be checked.

Just as you walk around your living space to see if everything is OK, you also need to "walk" around your home computer to see if there are any viruses lurking about. Most anti-virus programs let you schedule periodic exams of all files on your home computer on a regular basis, daily for example. If you leave your computer turned on over night, think about scheduling a full-system review during that time.

Some anti-virus programs have more advanced features that extend their recognition capabilities beyond virus signatures. Sometimes a file won't match any of the known signatures, but it may have some of the characteristics of a virus. This is comparable to getting that "there's something not quite right here, so I'm not going to let them in" feeling as you greet someone at your door. These heuristic tests, as they're called, help you to keep up with new viruses that aren't yet defined in your list of virus signatures.

An anti-virus program is frequently an add-on to your home computer, though your newly purchased computer might include a trial version. At some point, say after 60 days, you must purchase it to continue using it. To decide whether to make that purchase or to look elsewhere, use these steps for evaluating anti-virus programs:

1. The D**emand test:** Can you check a file on demand, for example, when you want to send an attachment as part of the KRESV tests?
2. The U**pdate test:** Can you update the virus signatures automatically? Daily is best.
3. The R**espond test:** What are all the ways that you can respond to an infected file? Can the virus checker clean a file?
4. The C**heck test:** Can you check every file that gets to your home computer, no matter how it gets there, and can those checks be automated?
5. The H**euristics test:** Does the virus checker do heuristics tests? How are these defined?

These tests – the **DURCH** tests – help you compare anti-virus programs. Once you've made your selection, install it and use all of its capabilities all of the time.

Intruders are the most successful in attacking all computers – not just home computers – when they use viruses and worms. Installing an anti-virus program and keeping it up to date is among the best defenses for your home computer. If your financial resources are limited, they are better spent purchasing a commercial anti-virus program than anything else.

To see an example that shows how to operate a virus checker, see http://www.fedcirc.gov/homeusers/HomeComputerSecurity/examples.html.

Task 2 - Keep Your System Patched

If one of your appliances broke, you'd probably try to have it repaired. You'd call a repairperson whom you hope could do the job. You'd get an estimate and then you'd either get it fixed or replace it. Your goal is to somehow restore the functions that the appliance provides.

What do you do when a software "appliance" – a program – or the operating system itself breaks? How do you restore the functions that they provide? Do you know whom to call or even where to look to determine what to do next?

Most vendors provide patches that are supposed to fix bugs in their products. Frequently these patches do what they're supposed to do. However, sometimes a patch fixes one problem but causes another. For example, did you ever have a repairperson fix an appliance but in the process, they scratched the floor or damaged a countertop during their visit? For a computer, the repair cycle might have to be repeated until a patch completely fixes a problem.

Vendors often provide free patches on their web sites. When you purchase programs, it's a good idea to see if and how the vendor supplies patches, and if and how they provide a way to ask questions about their products. Just as appliance vendors often sell extended warranties for their products, some software vendors may also sell support for theirs.

Have you ever received a recall notice for your car or another product you've purchased? Vendors send these notices to product owners when a safety-related problem has been discovered. Registering your purchase through the warranty card gives the vendor the information they need to contact you if there is a recall.

Program vendors also provide a recall-like service. You can receive patch notices through email by subscribing to mailing lists operated by the programs' vendors. Through this type of service, you can learn about problems with your computer even before you discover them and, hopefully, before intruders have the chance to exploit them. Consult the vendor's web site to see how to get email notices about patches as soon as they're available.

Some vendors have gone beyond mailing lists. They provide programs bundled with their systems that automatically contact their web sites looking for patches specifically for your home computer. These automatic updates tell you when patches are available, download them, and even install them. You can tailor the update features to do only want you want, such as just telling you something new is waiting but doing nothing more.

While the patching process is getting easier, even to the point where it can be completely automated, it is not yet foolproof. In some cases, installing a patch can cause another seemingly unrelated program to break. The challenge is to do as much homework as you can to learn what a patch is supposed to do and what problems it might cause once you've installed it.

This is a hard job. Often, the vendors don't tell you about problems their patches can cause. Why? Because it is simply impossible to test all possible programs with all possible patches to discover unexpected side effects. Imagine doing that job and then continuing to do that for each new program and patch that comes along. Vendors rely on their customers to tell them when something unexpected happens once a patch is installed. So, if this happens to you, let them know.

Imagine then that you've either found a patch on the vendor's site or you've received notice that a patch is available. What do you do next? Follow the steps below to evaluate a patch before you install it:

1. The A**ffected** test: Does this patch affect one of the programs on your computer? If it doesn't affect your computer, you're done. Whew!
2. The B**reak** test: Can you tell from the vendor's web site or the patch's description if installing it breaks something else that you care about? If installation does break something, then you have to decide how to proceed. Try notifying the vendor of the program that might break to learn what their strategy is for addressing this problem. Also, use your web browser to learn if anyone else has experienced this problem and what he or she did about it.
3. The U**ndo** test: Can you undo the patch? That is, can you restore your computer to the way it was before you installed the patch? Currently, vendors are building most patches with an uninstall feature that enables you to remove a patch that has unwanted consequences. In addition, some computers also come with features that help you restore them to a previously known and working state should there be a problem. You need to know what your computer provides so that you can undo a patch if necessary.

Recall from the Introduction that intruders exploit vulnerabilities to gain access to home computers. How do intruders find out about these vulnerabilities? In many cases, they read the same vendor mailing lists and use the same automatic notification schemes that you use. This means that you need to evaluate and install patches on your home

computer as soon as they're available. The longer a vulnerability is known, the greater the chances are that an intruder will find it on your home computer and exploit it. With the **ABU** tests, you can quickly evaluate and install patches to keep intruders off your home computer.

One last thing: patches are usually distributed as programs. This means that you need to use the DCAL steps described in Task 7, *Use Care When Downloading and Installing Programs,* before loading and installing a patch.

Intruders often take advantage of vulnerabilities wherever they may be. In many cases, the vulnerabilities they exploit may have patches, but those patches were not installed. For your home computer, make time to keep your programs patched wherever possible. If you can't patch a program, shop around for an equivalent program and use it until the original program is fixed or you've abandoned it in favor of something more reliable.

You can spend money on maintenance where you get patches for programs, but that's usually not necessary. Since most vendors provide free patches, mailing lists, and automatic updates, keeping your computer patched usually only costs you time.

To see an example that shows how to check for, download, and install patches, see http://www.fedcirc.gov/homeusers/HomeComputerSecurity/examples.html.

Task 3 - Use Care When Reading Email with Attachments

We've all heard stories about people receiving an item in the mail that in some way caused them harm. We've heard of letter bombs and exploding packages, and in 2001, we learned about Anthrax-laden letters. Although their frequency is low, they do make news.

These unsolicited items are sent to unsuspecting recipients. They may contain a return address, a provocative envelope, or something else that encourages its receiver to open it. This technique is called social engineering. Because we are trusting and curious, social engineering is often effective.

In the case of the Anthrax letters addressed to United States senators, the envelopes contained a school's return address as an inducement to open them. What government official wouldn't want to serve their constituency by reading and responding to a letter supposedly sent by a class at a school, especially an elementary school? By opening the letter and subsequently spreading its lethal contents, the recipient complied

with the wishes of the sender, a key foundation of social engineering. In the pre-Anthrax letter days, a mail handler might have given little thought to the contents of the letter or the validity of the return address. Those days are behind us.

You probably receive lots of mail each day, much of it unsolicited and containing unfamiliar but plausible return addresses. Some of this mail uses social engineering to tell you of a contest that you may have won or the details of a product that you might like. The sender is trying to encourage you to open the letter, read its contents, and interact with them in some way that is financially beneficial – to them. Even today, many of us open letters to learn what we've won or what fantastic deal awaits us. Since there are few consequences, there's no harm in opening them.

Email-borne viruses and worms operate much the same way, except there are consequences, sometimes significant ones. Malicious email often contains a return address of someone we know and often has a provocative Subject line. This is social engineering at its finest – something we want to read from someone we know.

Email viruses and worms are fairly common. If you've not received one, chances are you will. Here are steps you can use to help you decide what to do with every email message with an attachment that you receive. You should only read a message that passes all of these tests.

1. The **Know** test: Is the email from someone that you know?
2. The **Received** test: Have you received email from this sender before?
3. The **Expect** test: Were you expecting email with an attachment from this sender?
4. The **Sense** test: Does email from the sender with the contents as described in the Subject line and the name of the attachment(s) make sense? For example, would you expect the sender – let's say your Mother – to send you an email message with the Subject line "Here you have, ;o)" that contains a message with attachment – let's say AnnaKournikova.jpg.vbs? A message like that probably doesn't make sense. In fact, it happens to be an instance of the Anna Kournikova worm, and reading it can damage your system.

5. The **Virus** test: Does this email contain a virus? To determine this, you need to install and use an anti-virus program. That task is described in the section entitled *Install and Use Anti-Virus Programs*.

You should apply these five tests – **KRESV** – to every piece of email with an attachment that you receive. If any test fails, toss that email. If they all pass, then you still need to exercise care and watch for unexpected results as you read it.

Now, given the **KRESV** tests, imagine that you want to send email with an attachment to someone with whom you've never corresponded – what should you do? Here's a set of steps to follow to begin an email dialogue with someone.

1. Since the recipient doesn't already **Know** you, you need to send them an introductory email. It must not contain an attachment. Basically, you're introducing yourself and asking their permission to send email with an attachment that they may otherwise be suspicious of. Tell them who you are, what you'd like to do, and ask for permission to continue.
2. This introductory email qualifies as the mail **Received** from you.
3. Hopefully, they'll respond; and if they do, honor their wishes. If they choose not to receive email with an attachment from you, don't send one. If you never hear from them, try your introductory email one more time.
4. If they accept your offer to receive email with an attachment, send it off. They will **Know** you and will have **Received** email from you before. They will also **Expect** this email with an attachment, so you've satisfied the first three requirements of the KRESV tests.
5. Whatever you send should make **Sense** to them. Don't use a provocative Subject line or any other social engineering practice to encourage them to read your email.
6. Check the attachments for **Viruses**. This is again based on having virus-checking programs, and we'll discuss that later.

The **KRESV** tests help you focus on the most important issues when sending and receiving email with attachments. Use it every time you send email, but be aware that there is no foolproof scheme for working with email, or security in general. You still need to exercise care.

While an anti-virus program alerts you to many viruses that may find their way to your home computer, there will always be a lag between when a virus is discovered and when anti-virus program vendors provide the new virus signature. This means that you shouldn't rely entirely on your anti-virus programs. You must continue to exercise care when reading email.

Task 4 - Install and Use a Firewall Program

This section describes a firewall, its importance to your home computer strategy, and a way to think about the job you need to do. We're going to depart from our "computer-is-like-a-house-and-the-things-in-it" analogy to use another that you are probably also familiar with: an office building.

Have you ever visited a business where you first stopped at the reception desk to interact with a security guard? That guard's job is to assess everybody who wishes to enter or leave the building to decide if they should continue on or be stopped. The guard keeps the unwanted out and permits only appropriate people and objects to enter and leave the business's premises.

Let's dig deeper into this analogy. When someone enters a building, the security guard usually greets them. If they have an appropriate identification badge, they show it to the guard or swipe it through a reader. If all is OK, they pass through the guard's checkpoint. However, if something's wrong or if they are a visitor, they must first stop at the guard desk.

The guard asks whom they wish to see. The guard may also ask for identification such as a driver's license or their company ID. The guard reviews the list of expected guests to see if this person is approved to visit the party in question. If the guard decides everything is all right, the visitor may pass. The visitor usually signs a logbook with their name, the company they represent, whom they are seeing, and the time of day.

On a computer, the firewall acts much like a guard when it looks at network traffic destined for or received from another computer. The firewall determines if that traffic should continue on to its destination

or be stopped. The firewall "guard" is important because it keeps the unwanted out and permits only appropriate traffic to enter and leave the computer.

To do this job, the firewall has to look at every piece of information – every packet – that tries to enter or leave a computer. Each packet is labeled with where it came from and where it wants to go. Some packets are allowed to go anywhere (the employee with the ID badge) while others can only go to specific places (visitors for a specific person). If the firewall allows the packet to proceed (being acceptable according to the rules), it moves the packet on its way to the destination. In most cases, the firewall records where the packet came from, where it's going, and when it was seen. For people entering a building, this is similar to the ID card system keeping track of who enters or the visitor signing the visitor's log.

The building's guard may do a few more tasks before deciding that the person can pass. If the person is a visitor and is not on the visitors list, the guard calls the employee being visited to announce the visitor's arrival and to ask if they may pass. If the employee accepts the visitor, they may proceed. The guard may also give the visitor a badge that identifies them as a visitor. That badge may limit where in the building they can go and indicate if they need to be escorted. Finally, no matter whether the person is a visitor or an employee, the guard may inspect their briefcase or computer case before they pass.

The firewall can also check whether a given packet should pass, allowing the computer's user to respond to unanticipated network traffic (just as the guard does with the unexpected visitor). Individual packets can be allowed to pass, or the firewall can be changed to allow all future packets of the same type to pass. Some firewalls have advanced capabilities that make it possible to direct packets to a different destination and perhaps even have their contents concealed inside other packets (similar to the visitor being escorted). Finally, firewalls can filter packets based not only on their point of origin or destination, but also on their content (inspecting the briefcase or computer case before being allowed to pass).

Back to the office building, when employees leave the building, they may also have to swipe their ID card to show that they've left. A visitor signs out and returns their temporary badge. Both may be subject to having their possessions inspected before being allowed to leave.

Firewalls can also recognize and record when a computer-to-computer connection ends. If the connection was temporary (like a visitor), the firewall rules can change to deny future similar connections until the system's user authorizes them (just as visitors must re-identify themselves and be re-approved by an employee). Finally, outgoing connections can also be filtered according to content (again, similar to inspecting possessions at the exit).

What does this all mean? It means that with a firewall, you can control which packets are allowed to enter your home computer and which are allowed to leave. That's the easy part.

The hard part is deciding the details about the packets that are allowed to enter and exit your home computer. If your firewall supports content filtering, you also need to learn which content to allow and which not to allow. To help you get a handle on this harder task, let's return to our security guard analogy.

Imagine that you are that security guard and it's your first day on the job. You have to decide who's allowed in, who's allowed out, and what people can bring into and take out of the building. How do you do this?

One strategy is to be very conservative: let no one in or out and let no possessions in or out. This is very simple, very easy to achieve, but not particularly helpful to the business if none of its employees or visitors can get in or out. Nor is it helpful if they can't bring anything with them. With this type of strategy, your tenure as a security guard may be short-lived.

If you try this, you quickly learn that you need to change your strategy to allow people in and out only if they have acceptable identification and possessions using some agreed-to criteria. Add the requirement that if you don't meet the precise criteria for admittance, you don't get in.

With most firewalls, you can do the same thing. You can program your firewall to let nothing in and nothing out. Period. This is a deny-all firewall strategy and it does work, though it effectively disconnects you from the Internet. It is impractical for most home computers.

You can do what the security guard did: review each packet (employee or visitor) to see where it's coming from and where it's going. Some firewall products let you easily review each packet so that you can decide what to do with it. When you are shopping for a firewall, look for this review feature because it can be quite helpful. Practically speaking, it isn't easy to decide which traffic is all right and which is not all right.

Any feature that makes this job easier helps you achieve your goal of securing your home computer.

Just like the security guard who learns that anybody with a company photo ID is allowed to pass, you too can create firewall rules that allow traffic to pass without reviewing each packet each time. For example, you may choose to allow your Internet browsers to visit any web site. This rule would define the source of that traffic to be your browsers (Netscape Navigator and Microsoft Internet Explorer, for example) and the destination location to be any web server. This means that anybody using your home computer could visit any Internet web site, as long as that web server used the well-known standard locations.

Now that you have an idea of what your firewall security guard is trying to do, you need a method for gathering information and programming your firewall. Here is a set of steps to use to do just that:

1. The **Program** test: What's the program that wants to make a connection to the Internet? Although many programs may need to make the same type of connection to the same Internet destination, you need to know the name of each. Avoid general rules that allow all programs to make a connection. This often results in unwanted and unchecked behavior.
2. The **Location** test: What's the Internet location of the computer system to which your computer wants to connect? Locations consist of an address and a port number. Sometimes a program is allowed to connect to any Internet location, such as a web browser connecting to any web server. Again, you want to limit programs so that they only connect to specific locations where possible.
3. The **Allowed** test: Is this connection allowed or denied? Your firewall rules will contain some of each.
4. The **Temporary** test: Is this connection temporary or permanent? For example, if you're going to connect to this specific location more than five times each time you use the computer, you probably want to make the connection permanent. This means that you ought to add a rule to your firewall rules. If you aren't going to make this connection often, you should define it as temporary.

With each connection, apply the **PLAT** tests to get the information you need to build a firewall rule. The answer to the **PLAT** tests tells you if you need to include a new firewall rule for this new connection. For most firewall programs, you can temporarily allow a connection but avoid making it permanent by not including it in your rules. Where possible, allow only temporary connections.

As you run each program on your home computer, you'll learn how it uses the Internet. Slowly you'll begin to build the set of rules that define what traffic is allowed into and out of your computer. By only letting in and out what you approve and denying all else, you will strike a practical balance between allowing everything and allowing nothing in or out.

Along the way, you may come across exceptions to your rules. For example, you might decide that anybody who uses your home computer can visit any web site except a chosen few web sites. This is analogous to the security guard letting every employee pass except a few who need more attention first.

To do this with firewall rules, the exception rules must be listed before the general rules. For example, this means that the web sites whose connections are not allowed must be listed before the rules that allow all connections to any web site.

Why? Most firewall programs search their rules starting from the first through the last. When the firewall finds a rule that matches the packet being examined, the firewall honors it, does what the rule says, and looks no further. For example, if the firewall finds the general rule allowing any web site connections first, it honors this rule and doesn't look further for rules that might deny such a connection. So, the order of firewall rules is important.

Many firewalls can be programmed to require a password before changing the rules. This extra level of protection safeguards against unwanted changes no matter their source, that is, you, an intruder, or another user. Follow the guidance in Task 6, *Use Strong Passwords*, when assigning a password to your firewall.

Finally, make a backup of your firewall rules. You've probably taken a lot of time to build and tune them to match how your home computer is used. These rules are important to your computer's security, so back them up using the guidance in Task 5, *Make Backups of Important Files and Folders*.

Firewalls come in two general types: hardware and software (programs). The software versions also come in two types: free versions and commercial versions (ones that you purchase). At a minimum, you should use one of the free versions on your home computer. This is especially important if you have a laptop that you connect to your home network as well as a network at a hotel, a conference, or your office.

If you can afford a hardware firewall, you should install one of these too. We've recommended this as something to do later. (Firewall programs are task 4 on our list of recommended actions, and hardware firewalls are task 8.) The same issues apply to the hardware versions that apply to the software versions. Many can also be password protected against unwanted changes. Search the Internet with your browser to see what's available and what they cost. The price of hardware firewalls is coming down as the demand grows.

A firewall is your security guard that stands between your home computer and the Internet. It lets you control which traffic your computer accepts. It also controls which of your programs can connect to the Internet. With a firewall, you define which connections between your computer and other computers on the Internet are allowed and which are denied. There are free firewall products that provide the capabilities you need to secure your home computer. Commercial versions have even more features that can further protect your computer.

Firewalls are an important part of your home computer's security defenses. To see an example that shows how to operate a firewall, see http://www.fedcirc.gov/homeusers/HomeComputerSecurity/examples.html.

Task 5 - Make Backups of Important Files and Folders

Whether you know it or not, you've divided everything you own into two broad categories: those items you can replace and those you can't. For the items you can't replace, you've probably stored them in a safe place, either somewhere in your living space or elsewhere, in a lockbox at a bank, for example. In either case, you've probably also bought insurance that provides the funds you'd need to buy replacements. Your insurance policy covers almost everything you own.

On your home computer, have you similarly divided everything into the same categories? What have you done about the items – files in this case – that you can't replace? Examples are the files that make up your checking account records, that novel you've been writing for the past few years, and those pictures you took last summer with your digital camera. What happens if your computer malfunctions or is destroyed by a successful attacker? Are those files gone forever?

Now think about your car for a moment. Do you have a spare tire? Is it inflated? When was the last time you used it? Can you imagine buying a car without a spare tire? Even if you bought a used car without a spare, how soon did you buy a spare so that you'd have one when you needed it?

Think back to your home computer. Do you have a "spare tire," meaning a way to continue computing when you have a "blowout" caused by a malfunction or an intruder? Said another way, can you back up your files onto some other media so that you can recover them if you need to? If you'd never buy a car without a spare tire, why did you buy a computer without a device to back up your files?

When deciding what to do about backing up files on your computer, ask these questions:

1. The **Files** question: What files should you back up? The files you select are those that you can neither easily recreate nor reinstall from somewhere else, such as the CD-ROMs or the floppy disks that came with your computer.

   Be realistic. That check register you printed does not constitute a backup from which you can easily recreate the files needed by your checking account program. You're probably not going to re-enter all that data if the files are destroyed. Just as you protect your irreplaceable valuables, back up the files you cannot replace, easily or otherwise.

2. The **Often** question: How often should you back them up? In the best of all cases, you should back up a file every time it changes. If you don't, you'll have to reintroduce all the changes that happened since your last backup. Just as you store your precious jewelry in a lockbox at the local bank lest the lucky robber find it in your jewelry box, you need to store your files safely (back them up) after every use (change in the file) lest an intruder destroys the file or there's a system catastrophe.

3. The **Media** question: Where should you back them up to; that is, what media should you use to hold backed up files? The answer is: whatever you have. It's a question of how many of that media you have to use and how convenient it is. For example, most computers have a floppy disk drive. You could back up your irreplaceable files to floppies. That process just takes lots of time and may not be as convenient as using another media. Larger capacity removable disk drives and writable CD-ROMs also work well, take less time, and are more convenient.

   If you don't have a backup device, there are alternatives. There are Internet services that let you back up your files to another Internet computer. Some of these services provide "transparent access" to the backups. That is, they look like another hard drive attached to your computer. You use the file copy scheme that your computer provides to back up files and recover them from backed up storage. To find these services, do some Internet searches using your browser.

   Remember that the information you transfer across the Internet could be viewed and captured by others; that is, the information is in the clear. Be sensitive to that if you use an Internet-based backup computer. In addition, you need to be able to trust the information when you recover a file from that service.

4. The **Store** question: Where should you store that media once it contains your backed up files? No matter how you back up your files, you need to be concerned about where those backed up copies live.

   You already know that intruders try to break into your home computer to gain access to your files and your computer's resources. Another way to gain access to the same information is by stealing your backups. It is more difficult, though, since a robber must physically be where your backups are, whereas an intruder can access your home computer from literally anywhere in the world. The key is to know where the media is that contains your backed up files.

   Just like important papers stored in a fireproof container at your house, you also need to be concerned about your backups being destroyed if your living space is destroyed or damaged. This means that you ought to keep a copy of your backed up files in a fireproof container or somewhere beyond your living space, your office for example. It is the eternal compromise between security and usability. If you need to recover a file and the backed up copies are at the office, that's inconvenient. However, while storing them at home is more convenient and more usable, they

share the same risks that your computer faces should your living space be destroyed. Be aware of the issues and make a conscious decision, perhaps keeping copies in both places.

If you have that spare tire for your car or a lockbox for your valuables, you've already planned for the worst that can happen around your living space. Continue that good practice by backing up your critical files onto media that you can safely store elsewhere. Do those backups often enough that you can capture the changes you've made. With the **FOMS** questions, you have a structured approach to use to back up your critical files. You've now planned for the worst.

As you computerize the routine aspects of your daily life, making backup copies of important files and folders becomes critical. Even if you can't store the backup copies in a fireproof container or somewhere outside your home, make backups anyway. Any backup is better than none.

Task 6 - Use Strong Passwords

Your living space has doors and windows, and perhaps most of the time they're locked. For each lock that uses a key, chances are that each key is different. You know to lock up and not to share the keys with strangers, and probably not with most of your friends. You should not hide keys under the mat or in a flowerpot on your front porch.

Passwords for computers are much the same. For each computer and service you use (online purchasing, for example), you should have a password. Each password should be unique and unrelated to any of your other passwords. You shouldn't write them down nor should you share them with anyone, even your best friends.

Take a look at your front door key. It's pretty complicated. There are lots of notches and grooves. If there weren't so many possible variations, a thief could easily make a key for every possible combination and then try each on your front door. This trial-and-error method, (for computers, called brute force) is likely to be effective even if it takes a long time. Nonetheless, no matter how complicated, if the thief gets hold of your key, he or she can copy it and use that copy to open your door.

A password can also be complicated. Most schemes let you use any combination of letters, both upper and lower case, and numbers; and some also let you use punctuation marks. Lengths can vary. You can create a password to be as complicated as you want. The key (no pun intended) is to be able to remember this password whenever you need it without having to write it down to jog your memory.

Like the thief at your door, computer intruders also use trial-and-error, or brute-force techniques, to discover passwords. By bombarding a login scheme with all the words in a dictionary, they may "discover" the password that unlocks it. If they know something about you, such as your spouse's name, the kind of car you drive, or your interests, clever intruders can narrow the range of possible passwords and try those first. They are often successful. Even slight variations, such as adding a digit onto the end of a word or replacing the letter o (oh) with the digit 0 (zero), don't protect passwords. Intruders know we use tricks like this to make our passwords more difficult to guess.

Just like the front door key, even a complicated password can be copied and the copy reused. Remember the earlier discussion about information on the Internet being in the clear? Suppose that really strong password you took a long time to create – the one that's 14 characters long and contains 6 letters, 4 numbers, and 4 punctuation marks, all in random order – goes across the Internet in the clear. An intruder may be able to see it, save it, and use it. This is called sniffing and it is a common intruder practice.

The point is that you need to follow the practice of using a unique password with every account you have. Below is a set of steps that you can use to help you create passwords for your accounts:

1. The S**trong** test: Is the password as strong (meaning length and content) as the rules allow?
2. The U**nique** test: Is the password unique and unrelated to any of your other passwords?
3. The P**ractical** test: Can you remember it without having to write it down?
4. The R**ecent** test: Have you changed it recently?

In spite of the **SUPR** tests, you need to be aware that sniffing happens, and even the best of passwords can be captured and used by an intruder.

You should use passwords not only on your home computer but also for services you use elsewhere on the Internet. All should have the strongest passwords you can use and remember, and each password should be unique and unrelated to all other passwords. A strong password is a password that is longer than it is short, that uses combinations of uppercase and lowercase letters, numbers, and punctuation, and that is usually not a word found in a dictionary. Also remember that no matter how strong a password is, it can still be captured if an intruder can see it "in the clear" somewhere on the Internet. (See the *Information in the Clear* section.)

Task 7 - Use Care When Downloading and Installing Programs

When you buy an appliance, you give little thought to it doing you or your house any harm. Why? Because there are organizations like Underwriters Laboratories[2] that set standards and certify products. When you see a certifier's label, you have more confidence that a product will be safer than a competing product that does not carry the same label. You're willing to accept the risk because you believe the product has met some standards and has been certified by a respected authority.

Unfortunately, the Internet is not the same. There are neither standards nor many certification organizations. Anyone who writes a program can distribute it through any means available, such as through the web or by sending you a copy. Speaking of that, have you ever received a CD-ROM in the mail? How do you know that it contains what the label says? The answer is: you don't know. More importantly, it's difficult to know.

No matter how you acquire a program, it runs on your computer at the mercy of the program's author. Anything, any operation, any task that you can do, this program can also do. If you're allowed to remove any file, the program can too. If you can send email, the program can too. If you can install or remove a program, the program can too. Anything you can do, the intruder can do also, through the program you've just installed and run.

Sometimes there's no explanation of what a program is supposed to do or what it actually does. There may be no user's guide. There may be no way to contact the author. You're on your own, trying to weigh a program's benefits against the risk of the harm that it might cause.

What's the problem you're trying to solve here? You are trying to determine if the program you've just found satisfies your needs (say it provides a service that you want or you're just experimenting) without causing harm to your computer and ultimately the information you have on the computer. How do you decide if a program is what it says it is? How do you gauge the risk to you and your computer by running this program?

You address these same risk issues when you purchase an appliance; you may just not have realized that that's what you were doing. When you make that purchase, you buy from either a local store you know or a national chain with an established reputation. If there's a problem with your purchase, you can take it back to the store and exchange it or get your money back. If it causes you harm, you can seek relief through the legal system. The reputation of the merchant, the refund/return policy, and the availability of the legal system reduce your risk to a point where you make the purchase.

Apply these same practices when you buy a program. You should

- **Learn** as much as you can about the product and what it does before you purchase it.
- **Understand** the refund/return policy before you make your purchase.
- **Buy** from a local store that you already know or a national chain with an established reputation.

Presently, it is not as clear what the legal system's role is for a program that causes harm or does not work as advertised. In the meantime, the **LUB** practices are a good first step.

Today's Internet has a feature that standard products don't have, or at least have but to a lesser extent. This feature is free programs. There is a multitude of free programs available for all types of systems, with more available each day. The challenge is to decide which programs deserve your confidence and are, therefore, worth the risk of installing and running on your home computer.

So then, how do you decide if a program is worth it? To decide if you should install and run a program on your home computer, follow these steps:

1. The **Do** test: What does the program do? You should be able to read a clear description of what the program does. This description could be on the web site where you can download it or on the CD-ROM you use to install it. You need to realize that if the program was written with malicious intent, the author/intruder isn't going to tell you that the program will harm your system. They will probably try to mislead you. So, learn what you can, but consider the source and consider whether you can trust that information.
2. The **Changes** test: What files are installed and what other changes are made on your system when you install and run the program? Again, to do this test, you may have to ask the author/intruder how their program changes your system. Consider the source.
3. The **Author** test: Who is the author? (Can you use email, telephone, letter, or some other means to contact them?) Once you get this information, use it to try to contact them to verify that the contact information works. Your interactions with them may give you more clues about the program and its potential effects on your computer and you.
4. The **Learn** test: Has anybody else used this program, and what can you learn from him or her? Try some Internet searches using your web browser. Somebody has probably used this program before you, so learn what you can before you install it.

If you can't determine these things – the **DCAL** tests for short – about the program you'd like to install, then strongly consider whether it's worth the risk. Only you can decide what's best. Whatever you do, be prepared to rebuild your computer from scratch in case the program goes awry and destroys it. The section on backups (Task 5) tells you how to make a copy of your important information should you need it.

Your anti-virus program prevents some of the problems caused by downloading and installing programs. However, you need to remember that there's a lag between recognizing a virus and when your computer also knows about it. Even if that nifty program you've just downloaded doesn't contain a virus, it may behave in an unexpected way. You should continue to exercise care and do your homework when downloading, installing, and running new programs.

Task 8 - Install and Use a Hardware Firewall

Complement your firewall program by installing a hardware firewall. Together, these two firewalls stand between your home computer and the Internet. This is another place where your money is well spent.

Please go to Task 4, *Install and Use a Firewall Program*, to learn more about firewalls. That section concentrates primarily on firewall programs, but much of the information applies to hardware firewalls as well. To find out what hardware firewall products are available, search the Internet with your web browser.

Task 9 - Install and Use a File Encryption Program and Access Controls

Let's return to your living space and our original analogy. Think about your checkbook, your insurance policies, perhaps your birth certificate or passport, and other important documents you have at home. Where are they? They're probably stored in a filing cabinet or a safe, either of which that can be or is routinely locked. Why do you store these important items in a locked container?

Without realizing it, you are satisfying one of the three components of information security – confidentiality. Confidentiality means keeping secrets secret. Only those who are supposed to see that information should have access to it. You are keeping information sensitive to you and others away from those who should not be able to get to it, for example a family member or an intruder. By the way, the other two components of information security are integrity (Has my information changed?) and availability (Can I get to my information whenever I need it?).

You further protect information confidentiality when you enforce it by using an access control device, namely the lock on your filing cabinet or safe. This device stands between the information and those seeking access, and it grants access to all who have the combination, the key, or whatever tool unlocks the container. When several layers of access control devices are used (called "defense in depth") – you might also find that these containers are themselves in locked rooms. Would-be intruders must pass through several levels of protection before finally gaining access to the information they seek.

Now, think back to your home computer. The problem is to control access to files and folders. The access control device here is the access control list or ACL. ACLs define who can perform actions on a file or folder: reading and writing, for example. ACLs are equivalent to a locked filing cabinet for paper documents.

Different computer systems provide different types of ACLs. Some have fine-grained controls while others have virtually none. The key is to use all the controls that are available on your computer.

Frequently, vendors define ACLs that are overly permissive. This satisfies their need to ensure that access limitations don't get in the way of using their systems. Your challenge is to tighten those ACLs so that they properly restrict access to only those who need access. This means that you need to modify the ACLs from the settings set by the vendor. We'll talk more about how to do this shortly.

Returning to the home environment, do you remember a time when adults in your house wanted to say something to one another in front of their children but in such a way that the children couldn't understand what was being said? Perhaps they spelled their message or used Pig Latin (ig-pay Atin-lay) to conceal the meaning. This worked for a while, until the children learned to spell or could otherwise understand what was being said. What's really happening here?

Very simply, the adults could not control who could hear their conversation. It was inconvenient or perhaps impossible for them to go to another room where they couldn't be heard. They had to talk in a way that only those who knew the concealing scheme could understand what was being said.

On a computer, when access to information can't be limited, such for an e-commerce transaction over the Internet, that information is concealed through a mathematical process called encryption. Encryption transforms information from one form (readable text) to another (encrypted text). Its intent is to hide information from those who have neither the transformation method nor the particulars (the decryption keys) to transform the encrypted text into readable text. The encrypted text appears to be gibberish and remains so for people who don't have the scheme and the keys.

Back on the home front, the children eventually learned how to spell and perhaps also learned the trick to using Pig Latin. They can now understand the conversations the adults are having. While they could also understand the conversations held weeks, months, or even years before, the information in those conversations is no longer important. The encryption scheme – spelling or Pig Latin – is strong enough to guard the information during its useful lifetime.

Computer-based encryption schemes must also withstand the test of time. For example, if a credit card encryption scheme needs six months of computer time to break, the resulting clear text credit card number is probably still valid and, therefore, useful to an intruder. In this case, the encryption scheme isn't strong enough to guard the information for its entire useful lifetime.

So, to guard paper or computer files, you need to limit who has access to them by using the access control devices, whether filing cabinets and safes for paper or access control lists for information on a computer system. For assets whose access cannot be sufficiently limited, you need to encrypt them strongly enough so that the time it takes to decrypt them is longer than their useful life.

Now, what can you do?

First, if more than one person uses your computer, you can adjust the ACLs that control access to sensitive files and folders. Your goal is to allow the correct type of access to the files and folders that each user needs, and nothing more. The steps below help you to decide how to adjust the ACLs for files and folders:

1. The **Who** test: Who – which users – need access to files besides you?
2. The **Access** test: What type of access do they need? Read? Write?
3. The **Files/Folders** test: Which files and folders need special access? Just like your firewall rules, your general policy should be to limit access to only you first, and then grant access beyond that where needed.

By applying the **WAF** tests, you can limit access to sensitive files on your computer to only those who need it.

Setting proper ACLs is not a trivial task. Be prepared to repeat it a few times until you get it right for the way your computer is used. It's worth the time spent, but know that it may take longer than you expect.

For very sensitive files and for files that are on a laptop, don't rely solely on file and folder ACLs. You need to go further and use encryption.

Some vendors provide encryption with their systems right from the start. This means that all you have to do is follow the vendor's instructions on how to use those features, but be certain to use them.

On systems where encryption is not included, you need to install additional encryption programs. For encryption programs that you download from the Internet, be sure to follow the instructions in Task 7, *Use Care When Downloading and Installing Programs.* Also follow the instructions in Task 6, *Use Strong Passwords,* for additional guidance on passwords required by encryption programs.

There are free and commercial encryption programs, and in most cases, the free versions suffice. However, commercial programs may provide more features and may keep up better with newer and, therefore, stronger encryption methods. If you rely on a laptop computer, you should consider purchasing a commercial file encryption programs.

Whether paper files around your living space or files and folders on your computer, limit access where you can. On your computer, use encryption programs either when you can't restrict access to the extent that you'd like or when you want even more security protecting your computer files and folders.

To see examples that show how to use an encryption program and how to adjust ACLs, see http://www.fedcirc.gov/homeusers/HomeComputerSecurity/examples.html

Summary

Growing up, you learn many of the things you need to know about how to operate and care for a car by sitting in the back seat while adults drive and care for their vehicles. Similarly, you learn many of the things you need to know about how to care for and maintain a home by watching what is done to the one where you live. It is a slow, gradual process, so slow in fact you are probably unaware that you are learning the skills you need to do these same jobs yourself.

You don't have that same luxury of time to learn how to care for and operate your home computer. When you attach it to the Internet for the first time, it instantly becomes a target for intruders. You need to be ready right from the start.

As you grow up, you also learn that you need to spend time and money to repair and replace those things around your living space and your car that need your attention. You learn that you have to spend more time and more money to tailor them to meet your needs and to keep you and others safe during their use. You accept these responsibilities and their costs as part of the total cost of ownership of that car and living space.

Your home computer is much the same. There is the initial money that you pay to purchase that system. Then there are additional costs to tailor it and to keep you and the others who use your system safe. These additional costs are also your responsibility, and they are part of the total cost of ownership of your home computer.

This pamphlet helps you think about the problems you face when you have a home computer and gives you advice on how to address these problems. On the web, there are checklists and worksheets that help you keep track of important information about the steps you take to secure your computer, and a list of additional resources if you want to know more.

Checklists:

http://www.fedcirc.gov/homeusers/HomeComputerSecurity/checklists/checklist1-9.pdf

Additional Resources:

http://www.fedcirc.gov/homeusers/HomeComputerSecurity/index.html#resources

By taking the time to read this pamphlet, you know more about securing your home computer and the extra costs required to do this job. Do the tasks described here and share this pamphlet with your friends. We all benefit from a more secure Internet.

End Notes

1 *Where Wizards Stay Up Late: The Origins of the Internet* by Katie Hafner and Matthew Lyon. ISBN: 0684832674. Read a review at http://www.mantex.co.uk/reviews/hafner.htm.

2 The Underwriters Laboratories web site is http://www.ul.com/

Acknowledgments:

This pamphlet was designed and written by Lawrence R. Rogers (lrr@sei.cmu.edu). It was edited by Linda Hutz Pesante (lhp@sei.cmu.edu). The graphic design and illustrations were created by David Biber (dbiber@sei.cmu.edu). All work in the Networked Systems Survivability Program at Carnegie Mellon University's Software Engineering Institute in Pittsburgh, PA.