INTERNET SECURITY ALLIANCE

Common Sense Guide for Home and Individual Users

Recommended Actions for Information Security
1st Edition – February 2003

Internet Security Alliance Officers

Dr. Bill Hancock, Chairman, ISAlliance and Senior Vice President for Security, Cable & Wireless

Allan Woods, Past Chairman, ISAlliance and Vice Chairman and CIO, Mellon Financial Corp.

Doug Goodall, Vice Chairman, ISAlliance and CEO, RedSiren Technologies

John Shaughnessy, Vice Chairman, ISAlliance and Senior Vice President Visa, U.S.A.

Dave McCurdy, Executive Director, ISAlliance and President, Electronic Industries Alliance

Dr. Steve Cross, Deputy Executive Director, ISAlliance and Director, Software Engineering Institute, Carnegie Mellon University

Internet Security Alliance Board of Directors

AIG
Mellon
redsiren Security. Integrity. Trust.
Booz | Allen | Hamilton
NAM National Association of Manufacturers
Russell
CERIDIAN
NORTHROP GRUMMAN
SONY
CABLE & WIRELESS
NASDAQ
SINTEF Telecom and Informatics
NORSK TIPPING
TATA
IBM
NORTEL NETWORKS
VISA
ITT Industries Engineered for life
Raytheon
VeriSign

Internet Security Alliance Members

Automatic Data Processing
Boeing Company
Equant
Federal Express
Harris Corporation
Intuit
Merck
NEC
Riptech (Symantech)

Contents

Introduction

Why are home computers popular targets for intruders? Because they are easy to break into and intruders want to access information that is stored on hard drives such as credit card numbers and other financial account information. But it's not solely money-related information they're after. Intruders also want your computer resources, meaning hard disk space, fast processors, and Internet connections. They use these resources to attack other computers on the Internet. The more computers an intruder uses, the harder it is for anyone, including law enforcement, to determine where the attack is 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. Intruders can quickly locate and attack them, particularly those with high-speed Internet connections (cable modems and DSL modems) that are always turned on. Regardless of how a home computer accesses the Internet, intruders' attacks are often successful. Many home computer users don't realize that they need to become more aware of computer security. Just as a car owner is responsible for having insurance when driving a car, a user has a comparable responsibility for a home computer's security, particularly when connected to the Internet. This guide recommends actions you, as a home user, can take to improve the security of your home computer. The goal is to keep intruders and their programs from invading yours. Remember, when you're connected to the Internet, the Internet is connected to you.

How do intruders break into home computers? In some cases, they send email with a virus. Reading this email activates the virus, creating a "foot in the door" that an intruder can use to access the computer. In other cases, they take advantage of a flaw or weakness in a software program stored on the computer – a vulnerability – to gain access. In addition, popular applications software (such as media players) and the files they produce (such as Word documents and Excel spreadsheets) can contain viruses when downloaded from an untrustworthy source or updated with bogus patches.

Once they're on a home computer, intruders can install new programs that let them continue to use the computer – even after the user plugs the holes the intruder took advantage of to get onto the computer in the first place. These "backdoors" are often cleverly disguised so that they blend in with other programs and are hard to detect.

Whether the computer runs Microsoft® Windows®, Apple's Mac OS, Linux, or another operating system, the actions you need to take to better secure your home computer are the same and will remain so as new versions of the system are released. Every home user has a responsibility to understand the security-related issues that should be addressed on their computers.

The actions in this guide are a summary of more detailed material developed for the General Services Administration's FedCIRC (Federal Computer Incident Response Center) by the CERT/CC® at Carnegie Mellon University [1]. This material is available at both http://www.fedcirc.gov/homeusers/HomeComputerSecurity/ and http://www.cert.org/homeusers/HomeComputerSecurity/. Consult the Webopedia Online Dictionary for Computer and Internet Terms at http://www.webopedia.com for the definition of technical terms that are not familiar to you.

Two Useful Things to Know

1. 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 and the mail we receive. We trust our parents, our partner or spouse, our children, and our co-workers. In fact, those who don't trust are often thought to be cynical.

So our natural inclination when using the Internet is to trust the content of the web sites we visit and the email we receive, particularly if it appears to be sent from someone we know. However an intruder can easily falsify where an email message comes from. This information forging – called spoofing – 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 another computer on the Internet should not be trusted automatically and unconditionally. When you trust an email message that has a harmful virus attached to it, your computer can be infected, files destroyed, and work lost. Having a realistic sense of insecurity is better than a false sense of security. So you need to think about the information you trust and be critical, cautious, and a bit paranoid.

2. Information in the Clear

When you send email, browse a web site, or chat online with someone, the conversation does not go directly from your computer to the recipient's computer. Instead, it goes from your computer to another computer to still another computer and so on, eventually reaching the final destination. Think of all of these computers as an Internet "room."

Anyone, or more accurately, any software program, in that Internet room that can hear this "conversation" can also probably understand it. Why? Because most Internet conversations are in the clear, meaning that the information exchanged between computers is in easily decipherable strings of characters, that is, the information is not concealed or hidden in any way. The information sent across the Internet may be at risk of others listening in; they can capture what a user sends and use it for their own benefit.

Refer to the guidelines in Action 9, Encryption as one means for addressing this problem. Encryption uses mathematics to scramble information. There are many programs you can install to encrypt the information you send across the Internet, should you need to do so.

In the guidelines that follow, you will see that the conditions of trust and information in the clear serve as the basis for many of the recommendations.

Securing Your Home Computer

This guide presents nine actions that home users can take to better secure their home computers, seven designated as basic and two as more advanced. The actions are in the order that addresses the most-often used intruder attack methods, starting with viruses. More detailed guidance for each action, along with operating-system-specific examples, is available at http://www.cert.org/homeusers/homecomputersecurity.html.

Basic

Action 1 Install and Use an Anti-Virus Program (the DURCH tests)

Intruders have the most success attacking any computer – including a home computer – when they use viruses and worms as the means for gaining access. Installing an anti-virus (AV) program and keeping it up to date are among the best defenses. If financial resources are limited, they are better spent purchasing a commercial anti-virus program than anything else described in this guide.

AV programs look at the contents of each file, searching for specific characters that match a profile or pattern – called a virus signature – known to be harmful. For each file that matches a signature, an AV program typically provides several options, such as removing the offending patterns or destroying the file that contains the virus.

When AV program vendors learn about a new virus, they provide an updated set of virus signatures that include the new one. Through a home user's actions or through automated features provided by the AV program, the home computer learns of this new virus and begins checking each file for it's occurrence, along with checking for the presence of any older viruses.

You often have the opportunity to decide what to do when a virus has been discovered on your computer. Depending upon the specific characteristics of the virus, you might clean the infected file with the help of the AV program. Or you might be forced to destroy the file and load a new copy from backups or original distribution CDs that came from the vendor when you originally purchased the computer. Your options depend upon the choice of AV program and the virus that's been detected.

Viruses can infect a home computer in many ways: through floppy disks, CDs, email, web sites, and downloaded files. You need to check all of these for viruses each time they are used. In other words, when you insert a floppy disk, receive email, or download a file, you need to check for viruses. An AV program may provide an option to specify all of these as places to be checked for viruses each time they are accessed. Some AV programs do this automatically. If so, all you need to do is open or run the file to cause it to be checked.

Most AV programs provide an option to schedule periodic examinations of all files on a regular basis, such as daily. If you leave your computer turned on over night, the AV program can perform a full-system virus scan during this time.

[more advanced] Some AV programs have more advanced features that extend their recognition capabilities beyond known virus signatures. Sometimes a file won't match any of the current signatures, but it may have some of the characteristics of a virus. These heuristic tests, as they're

called, help a user to keep up with new viruses that aren't yet defined in the current list of virus signatures provided by the vendor. Heuristic tests can slow down performance.

Often an AV program is not installed on a new computer, although some computer vendors may include a trial version of some AV vendor's product. At some point, say after 60 days, you must purchase it to continue using it. Consider using these tests to evaluate which AV program to purchase and install:

The **Demand** test: Can the AV program check a file on demand, for example, when you want to send an email attachment and want to make sure that the attachment does not have a virus?
The **Update** test: Can you update virus signatures automatically to add the latest known viruses? If so, we recommend enabling this feature. Daily is best. If this feature is not available, perform signature updates manually, also on a daily basis.
The **Respond** test: What are the ways that you can respond to a notification of an infected file? Can the AV program clean the file, eliminate the virus, and repair the damage the virus did?
The **Check** test: Can the AV program check every file that comes into your home computer, no matter how it gets there, and can these checks be automated? Note that some vendors turn off automated checking to make installation easier, so you need to enable this feature if it is turned off.
The **Heuristics** test: Does the AV program do heuristics tests? How are these defined?

The **DURCH** tests can help you to compare the capabilities of several AV programs and make a better purchase decision.

Action 2 Keep Your System Patched (the ABU tests)

What should you do when a software program or the operating system (the program that runs the computer) breaks or begins operating erratically? How can you find out whom to call or where to look to determine what to do next? How do you restore the features that the program used to provide that no longer work?

Most software vendors provide patches that are supposed to fix problems in their products. Frequently these patches do what they're supposed to do. However, sometimes a patch fixes one problem but creates another. When this happens, the repair cycle may have to be repeated until a number of successive patches completely fix a problem.

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

Software vendors often provide a recall-like service, similar to receiving a recall notice for your car. You can receive patch notices through email by subscribing to mailing lists operated by the vendor. Through this type of service, you can learn about potential problems before they occur 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 provide programs (installed on a home computer) that automatically contact the vendors' web sites looking for new patches to their software. These programs can tell you when patches are available, and can download and install them. You tailor the program's update features to do only what you want, for example, reporting that a new patch is available but giving you the option to defer its download and installation.

While software patching 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 learn what a patch is supposed to do and what problems it might cause once installed. This is not easy. Often a vendor doesn't report what problems their patches can cause. Why? Because it is simply impossible to test all programs with all patches to discover unexpected side effects. Vendors rely on their customers to tell them when something unexpected happens once a patch is installed. So if you run into this problem, make sure to let your vendor know.

Conduct these tests to evaluate a patch before installing it:

The **A**ffected test: Does this patch affect one of your home computer's programs? If not, you're done.
The **B**reak test: Does the vendor's web site or patch description indicate if installing the patch breaks something else? If installation does affect another program, then you have to decide how best to proceed. Try notifying the vendor of the program that might break to learn what their strategy is for addressing this problem. Consider using your web browser's search feature to learn if anyone else has experienced this problem and what he or she did about it. You can also decide not to install the patch, accepting the risk that comes with this.

The **Undo** test: Can you undo the patch? That is, can you restore the computer to the way it was before the patch was installed? Currently, vendors are building most patches with an uninstall feature that allows you to remove a patch that has unwanted consequences. In addition, some computers 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 vendor provides so that you can undo a patch if necessary.

As stated in the Introduction, intruders use 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 services 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 lower the odds that intruders will attack your home computer.

Keep in mind that patches are usually distributed as programs. This means that you need to use the **DCAL** tests described in Action 7, Use Care When Downloading and Installing Programs, before loading and installing a patch.

Take the 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.

Action 3 Use Care When Reading Email with Attachments (the KRESV tests)

You probably receive mail delivered by the US Postal Service every day. Much of it is unsolicited and contains unfamiliar but plausible return addresses. Some of this mail uses inducements (called 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 mail, 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 generally no harm in opening them. However, some of these offers are fraudulent so a certain amount of caution is required if responding

The same is true for email – some messages may contain viruses or worms that can cause significant problems for you and others. Malicious email often contains a return address of someone you know and often has a provocative Subject line. This is social engineering at its finest – something you want to read from someone you know.

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

The **Know** test: Is the email from someone that you know?
The **Received** test: Have you received email from this sender before?
The **Expect** test: Were you expecting email with an attachment from this sender?
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? This message 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.
The **Virus** test: Does this email contain a virus? This is described in Action 1, Install and Use an Anti-Virus Program.

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

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 are some steps to follow to begin an email dialogue with someone new:

Since the recipient doesn't **Know** you, consider sending them an introductory email. It must not contain an attachment. This email introduces you and asks their permission to send email with an attachment. Tell them who you are, what you'd like to do, and ask for their permission to continue.

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.
If they accept your offer to receive email with an attachment, send it. They now **Know** you and have **Received** email from you before. They also **Expect** this email with an attachment, so you've satisfied the first three **KRESV** tests.
Whatever you send should make **Sense** to them. Don't use a provocative Subject line or any other social engineering techniques to encourage them to read your email.
Check any attachments for **Viruses**. This is done using an AV program that scans outgoing email and attachments (see Action 1).

The **KRESV** tests help you to address the key issues when sending and receiving email with attachments. However, keep in mind that no solution is 100 percent foolproof. There is always a time lag between when a virus is discovered and when your AV program vendor provides the new virus signature that you then find out about and install. Don't rely entirely on your AV program; continue to exercise care when reading email.

Action 4 Install and Use a Firewall Program (the PLAT tests)

A firewall performs much the same job as a security guard at a public building. It examines the messages coming into your home computer from the Internet as well as the messages you send out. The firewall determines if these messages should continue on to their destination or be stopped. The firewall "guard" is important because it keeps the unwanted out, permitting only appropriate messages to enter and leave your home 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 (like an employee with a general access ID badge for the entire building) while others can only go to designated places (like visitors coming to see a specific person in the building). If the firewall allows the packet to proceed (accepted according to defined 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 an ID card system that keeps track of who enters or a 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 enter. If the employee accepts the visitor, they 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 an escort. 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 messages (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 to direct packets to a different destination and perhaps even have their contents concealed inside other packets (similar to a 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).

When employees leave the building, they may have to swipe their ID card through a card reader 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 computer's user authorizes them (just as visitors must re-identify themselves and be re-approved by an employee). Finally, the content of outgoing messages can also be reviewed and actions taken based on 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 defining the rules as to which packets 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 the 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. 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 condition 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. This is a *deny-all* firewall strategy and it does work, though it effectively disconnects you from the Internet. It is an impractical solution for most users.

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 acceptable and which is not. 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 can create firewall rules that allow packets 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 these packets to be your browsers (Netscape Navigator or Microsoft Internet Explorer, for example) and the destination location to be any web server.

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

The **Program** test: What program(s) on your home computer 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.
The **Location** test: What is 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 site. Again, you want to limit programs so that they only connect to specific locations where possible.
The **Allowed** test: Is this connection allowed or denied? Your firewall rules will contain some of each.
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 this connection permanent. So add a rule to your firewall rules. If you aren't going to make this connection often, define it as temporary.

With each connection, apply the **PLAT** tests to get the information you need to build a firewall rule. The answers to the **PLAT** tests tell 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 learn how it uses the Internet. Slowly you begin to build the set of rules that define what packets are allowed into and out of your computer. By letting in and out only what you approve and denying everything else, you 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 with the first rule and continuing 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 attempted by you, an intruder, or another user. Follow the guidance in Action 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 you use your home computer. These rules are important to your computer's security so back them up using the guidance in Action 5, Make Backups of Important Files.

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 to 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 as a more advanced action (see Action 8, Install and Use a Hardware Firewall). 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 decreasing as the demand grows.

A firewall is your security guard that stands between your home computer and the Internet. It lets you control which messages your computer accepts. It also controls which of your programs can connect to the Internet. With a firewall, you define the rules.

Action 5 Make Backups of Important Files and Folders (the FOMS tests)

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 in a lockbox at a bank. In either case, you've probably 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 these same two categories? What have you done about the items – files in this case – that you can't replace? Examples are the files containing your financial records, that novel you've been writing for the past few years, and pictures you took last summer with your digital camera. What happens if your computer malfunctions or is destroyed by an intruder? Are these files gone forever? Do you have a way to continue working on important computer files when you have a malfunction or an intruder attack? Do you copy your files onto some other media (like a disk or CD) so that you can recover them if you need to?

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

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 CDs or the 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.
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 re-enter all of the changes that occurred since your last backup if anything happens.
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 disk drive. You could back up your irreplaceable files on disks. This process just takes lots of time and may not be as convenient as using another media. Larger capacity removable disk drives and writable CDs (CD-RW or CD ReWritable) 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-accessible 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 feature that your computer provides to back up files and recover them from backed up storage. You need to consider the speed of your Internet connection, given the volume of data you intend to transfer, and the storage capacity the provider is able to provide. To find these services, do an Internet search using your browser. However, make sure you are dealing with a reputable service provider to ensure that the organization is viable, the service is not a scam, and that your information is being adequately protected.

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 this 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 this service provider.
The **Store** question: Where should you store the media once it contains your backed up files? No matter how you back up your files, you need to be concerned about where backed up copies live. And make sure to overwrite, erase, or destroy the media if it contains sensitive information that you no longer need.

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 thief must physically be where your backups are, whereas an intruder can access your home computer from any network connection 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 outside 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, this is inconvenient. However, while storing them at home is more convenient, they share the same risks as your computer should your living space be destroyed. Be aware of the issues and make a conscious decision, perhaps keeping copies in both places.

With the **FOMS** questions, you have a structured approach to backing up your critical files. As you computerize the routine aspects of your daily life, making backup copies of important files and folders becomes important. 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.

Action 6 Use Strong Passwords (the SUPR tests)

Your living space has doors and windows, and let's say they're typically 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 or share them with anyone. But if you do need to write them down, make sure the record is stored in a secure location such as a locked file cabinet.

Your front door key is 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 the copy to open your door.

A password can also be complicated. You can often use any combination of letters, both upper and lower case, numbers, and punctuation marks. Lengths can vary (a minimum of six characters; longer is better). You can create a password to be as complicated as you want. The key 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 use trial-and-error, or brute-force techniques, to discover passwords. By bombarding a login program 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 from discovery.

Just like the front door key, even a complicated password can be copied and reused. The strong password you just created – 14 characters long and contains 6 letters, 4 numbers, and 4 punctuation marks, all in random order – most likely travels 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. You need to follow the practice of using a unique password with every account you have.

Below are some tests to help you create better passwords:

The **S**trong test: Is the password as strong (meaning length and content) as the rules allow?
The **U**nique test: Is the password unique and unrelated to any of your other passwords?
The **P**ractical test: Can you remember it without having to write it down?
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, so make sure to change them regularly.

Action 7 Use Care When Downloading and Installing Programs (the LUB and DCAL tests)

Anyone who writes a software program can distribute it on the Internet through the web or by sending you a copy attached to an email. Have you ever received a CD in the mail? How can you be certain that it contains what the label says? A newly acquired program runs on your computer at the mercy of the program's author. Any task that you can do on your computer, this program can also do. If you delete a file, send email, or add or remove a program, your newly installed program can do this too. And an intruder can do these tasks unbeknownst to you, through the program you've just installed and run.

Programs occasionally come with no explanation of what they do. 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.

When you are considering buying a software program, you need to do the best you can to determine if the program satisfies your needs without causing harm to your computer or the information on it (your files and other programs). How do you decide if a program is what it says it is and provides the service you are seeking? How do you gauge the risks of running this program?

Apply these practices before purchasing a software program:

Learn as much as you can about the program and what it does before you buy it.
Understand the refund/return policy before you make your purchase.
Buy from a vendor that has an established reputation or that has been recommended by trusted sources, either online or by visiting the store.

Currently, the legalities associated with a purchased program that causes harm or does not work as advertised are unclear. In the meantime, the **LUB** practices are a good first step.

In addition to purchased software, there is a multitude of free programs available on the Internet for all types of systems, with more available each day. The challenge is to decide which programs are reputable and are, therefore, worth the risk of installing and running them on your home computer. To decide if you should install and run a program on your home computer, perform these tests:

The **D**o test: What does the program do? A clear description of the programs features and any problems that it may cause should be accessible on the web site where you can download it or on the CD you use to install it. 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 trust this information.
The **C**hanges test: What files are installed and what other changes are made on your system when you install and run the program? Read the description, or you may have to ask the author/intruder how their program changes your system. Consider the source.

The **A**uthor test: Who is the author? Can you use email, telephone, letter, or some other means to contact them? Once you get this information, try to contact them to verify that the contact information works. Your interaction may give you more clues about the program.
The **L**earn test: Has anyone else used this program, and what can you learn from them? Try some Internet searches using your web browser. Somebody has probably used this program, so learn what you can before you install it. And make sure there are no hidden charges.

If you can't perform the **DCAL** tests on 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. Action 5, Make Backups of Important Files and Folders tells you how to make a copy of your important information should you need it.

It may be necessary to disable your anti-virus software when installing a new program due to compatibility issues but only do this if necessary. Make sure to re-enable your AV software after the new program installation is complete.

Your anti-virus program (Action 1) can prevent some (but not all) of the problems caused when downloading and installing programs. However, remember that there is a time lag between the vendor recognizing a new virus and when your computer's AV program is able to check for it after downloading the new signature. 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.

More Advanced

Action 8 Install and Use a Hardware Firewall

Complement your software firewall program by installing a hardware firewall. Together, these two firewalls stand between your home computer and the Internet. Refer to Action 4, Install and Use a Firewall Program to learn more about firewalls. This Action concentrates primarily on software firewalls, but much of the information applies to hardware firewalls. To find out what hardware firewall products are available, search the Internet with your web browser.

Action 9 Install and Use a File Encryption Program and Access Controls (the WAF tests)

Confidentiality is one of the three major principles of information security. [The other two are *integrity* (Has my information changed?) and *availability* (Can I get to my information whenever I need it?)] Confidentiality means keeping secrets secret. Only those who are supposed to see confidential information have access to it; others can't get to it.

One way to protect the confidentiality of information in general is to use an access control device, such as a lock on your file cabinet or safe. This device stands between the information and those seeking access, and it grants access to those who have the combination or the key, and no one else. When several types of access control devices are used (such as placing the locked file cabinet in a locked room), would-be intruders must pass through several levels of protection to gain access to the information they seek, which is much tougher.

For your home computer, you want to control access to files and folders. The primary access control device is the access control list, or ACL. ACLs define who can perform actions on a file or folder such as reading and writing. Using ACLs is equivalent to having a locked file cabinet for paper documents. Different computer systems provide different types of ACLs. Some have very detailed controls[1] while others have very few. You'll want 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 these 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.

By way of an analogy, do you remember a time when adults wanted to say something to one another in front of their children such 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 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 not possible to go to another room where they couldn't be heard. They had to talk so that only those who knew the translation scheme could understand what was being said.

On a computer, when access to information can't be limited, such as for a credit card transaction over the Internet, this information can be concealed through a mathematical process called encryption. Encryption transforms information from one form (readable text) to another (encrypted or scrambled text). Its intent is to hide information from those who don't have the need to know. The encrypted text appears to be gibberish and remains so for people who don't have the encryption transformation scheme and the decryption keys to turn the encrypted text back into readable text.

[1] such as read, read-only, write, write-add, write-update, execute, execute-only, create, rename, delete, change, access, none.

To be effective, computer-based encryption schemes must protect the information they encrypt for a period of time that exceeds the useful life of the information. For example, if a credit card encryption scheme can be broken in six months of computer processing time, the decrypted credit card number is probably valid (still in use by the credit card owner) and, therefore, still 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: file cabinets and safes for paper or access control lists for information on a computer system. For assets to which 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.

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 permit access to the files and folders that each user needs, and nothing more.

The tests below help you to decide how to define the ACLs for files and folders:

The **Who** test: Who – which users – need access to files besides you?
The **Access** test: What type of access do they need? Read? Write? Modify? Delete?
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 specific access to other users, where needed.

By applying the **WAF** tests, you can limit access to sensitive files 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. Just follow the vendor's instructions.

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

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

Other Useful Actions [2]

Remove file and printer sharing in your computer, particularly when accessing the Internet using cable modems, digital subscriber lines (DSL), or other high-speed connections.
Do not select the option on web browsers for storing or retaining user name and password.
Do not disclose personal, financial, or credit card information to little-known or suspect web sites.
Delete spam and chain emails; do not forward these and do not use the unsubscribe feature.
Log off the online session and turn off your computer when it is not in use.
Do not use a computer or a device that cannot be fully trusted.
Do not use public or Internet café computers to access online financial services accounts or perform financial transactions.
Ensure your browser supports strong encryption (at least 128-bit). Most browsers now provide this by default.

Summary

You learn much of what you need to know about how to operate a car by watching how it's done (before you are old enough to drive). 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 and helping out. Learning about home and car care is a slow, gradual process.

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 learn that you need to spend time and money to repair and replace your possessions. You often 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 the 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 your responsibility, and they are part of the total cost of ownership of your home computer.

This guide helps you think about the problems you face when you have a home computer and gives you advice on how to address these problems. By taking the time to read this guide, you know more about securing your home computer and the extra costs required to do this job. Take the actions described here and share this guide with your friends. Remember, when you're connected to the Internet, the Internet is connected to you. We all benefit from a more secure Internet.

References and Additional Resources

[1] Rogers, Larry. "Home Computer Security." This work was produced for FedCIRC and the General Services Administration by the CERT® Coordination Center, Software Engineering Institute, Carnegie Mellon University, 2002. Available at http://www.fedcirc.gov/homeusers/HomeComputerSecurity/ and http://www.cert.org/homeusers/homeusersecurity.html

[2] Monetary Authority of Singapore. "Technology Risk Guidelines for Financial Institutions, Draft for Comments." November, 2002.

Other resources on the topic of home computer security:

Home Network Security; http://www.cert.org/tech_tips/home_networks.html
The National Strategy to Secure CyberSpace, Draft, September, 2002; http://www.whitehouse.gov/pcipb
Security for Telecommuting and Broadband Communications, Special Publication 800-46, September 2002; http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf
Stay Safe Online; http://www.staysafeonline.info

Other CERT/CC articles, available at http://www.cert.org/homeusers/:
Attack Scenarios: How to Get There from Here December 2001
Email: A Postcard Written in Pencil June 2001
File Cabinets and Pig Latin: Guards for Information Assets May 2002
Internet: Friend or Foe? January 2002
Is There an Intruder in my Computer? February 2002
Yesterday I Couldn't Spell Administrator; Now I Am One! September 2001

Authors

Lawrence R. Rogers, Senior Member of the Technical Staff, Carnegie Mellon University, Software Engineering Institute

Julia H. Allen, Senior Member of the Technical Staff, Carnegie Mellon University, Software Engineering Institute

Contributors

Susan Grant, Vice President, Public Policy, National Consumer League
Tom Kellermann, Data Risk Management Specialist, Financial Sector Strategy and Policy, The World Bank
Yoram Maliniak, Director, Knowledge Management and Information Security, Raytheon Co.
John Shaughnessy, Senior Vice President, Visa USA
Don Skillman, Director of Internet Policy, ISAlliance

Topics to Address with Your Internet Service Provider

Policies

- Where can I find your policy for using my Internet connection in terms of things I am permitted to do and things I am prohibited from doing?

Contacting and Getting Help from My ISP

- What is your technical support contact information (telephone number, email address) and hours? Can I use this contact information for security concerns?
- How long does it typically take your technical support organization to respond to security questions?
- What can I expect when I call (level of service)?

General Home Computer Security

- Do you provide security recommendations to your customers?
- What practices, procedures, or technology do you require of your customers?
- Do you recommend any security products? Have you negotiated preferred pricing on any security-related products?

My Internet Connection

- Do you restrict any connections to my home computer and if so, which connections?
- Do you restrict any connections from my home computer and if so, which connections?
- Do you provide the capability to deny access to specific web sites that I can select for blocking?
- Do you monitor your networks looking for known intrusions, including viruses in email and web traffic?

Responding to Breakins and Breakin Attempts

- If my home computer is broken into or is the target of an attack, what can you do to help me understand what happened and how to recover from it?
- Have you worked with any law enforcement organizations on any security events before?

If You Use Your ISP's Mail Service

- What type of spam filtering do you provide? How do I inform you of spam email that I receive?
- Do you provide the capability to filter email from unsolicited or undesired sites?
- Do you monitor the content of email attachments for viruses and other malicious software and block those that are suspicious?
- Do you provide your customer list and email addresses to other organizations?

Topics to Address with Your Financial Institution and Credit Card Provider

General user questions and guidelines:

- How do you protect the privacy of my personal information and transactions?
- Do you provide your customer list and email addresses to other organizations?
- Do you have a Frequently Asked Questions (FAQ) or any other resources that can help me to understand how to use the Internet and my web browser more securely when buying items over the Internet?
- What is my liability if an unauthorized party captures my credit card number online and starts using it?
- Check the authenticity of the Provider's web site by comparing the URL and the Provider's name in its digital certificate [2]
- Check that the Provider's web site address changes from http:// to https:// and that a security icon that looks like lock or key appear when authentication and confidentiality are expected [2]
- Check account balances and transactions frequently; immediately report any discrepancies [2]

Groundrules for PINs (Personal Identification Numbers) that your Provider should enforce:

- At least 6 digits or 6 alphanumeric characters in length and does not use the same digit or character more than twice
- Not be based on user id, telephone number, birthday, other personal information, or any word from a dictionary
- That you change a PIN regularly

User guidelines for PIN use: [2]

- Be kept confidential at all times, not divulged to anyone, and not written down
- The same PIN should not be used for different websites, applications, or services, particularly when they relate to different entities