San Jose
Mercury News
April 30, 1995

ILLUSTRATION. WES KILLINGBECK–MERCURY NEWS

Computer Protection

General tips

1. Back up your computer's data at least once a week. Keep a copy of a recent backup at a site other than where you keep your computer; if there's a fire you'll lose everything.

2. Be sure that your name, telephone number and address are engraved on your computer or written with an indelible marker.

3. Write down your computer's serial number as an additional anti-theft measure. Be sure to keep it at a different location than the computer itself.

4. Get a lock for your computer. Use it.

5. Make sure your insurance is up to date.

If you use a laptop:

1. Make a complete backup of your laptop before taking it on a trip. Then, if your computer is lost, stolen or damaged, you will only lose the work that you've done while traveling.

2. Write your name and phone number on your laptop with an indelible marker, so that it can be easily returned if you lose it (and an honest person finds it). Your name will also make it easier for police to return your laptop if it's stolen and recovered.

3. If your laptop is under warranty or covered by an extended service plan, keep a copy of your warranty paperwork when you travel in the event that you need service. Also bring a copy of the manufacturer's service and support numbers.

A GUIDE TO SAFER COMPUTING

HOW TO BACK UP YOUR DATA, KEEP YOUR HARDWARE SECURE

BY SIMSON GARFINKEL
Special to the Mercury News

DESPITE the recent rash of publicity surrounding malicious computer hackers and government wiretappers, most computer users today should be concerned with more mundane threats.

You're much more vulnerable to losses from accidents, disk crashes and burglars than from some clever network snoop. From backups to encryption to plain old common sense, you can lessen the chances of losing your data or your machine, security experts say.

You can replace a stolen computer. You're in trouble if you can't replace data, no matter how you lose it.

Backups protect the information on your computer from hardware failure, theft and your own errors, such as accidentally deleting your electronic checkbook. In all of these cases, it is important to be able to reconstruct all of your computer's files from the backup diskettes or tapes.

For that reason, "Backing up your system regularly and keeping the backups in a safe place" is a vital part of your computing routine, says Eugene Spafford, a professor of computer science at Purdue University who specializes in computer security.

Backups are such a simple thing to do: At the very least, copy your important files to floppy disks. People with today's larger hard disks should consider investing in a tape drive, so that the computer's entire hard disk can be saved at the same time on a single tape or several tapes rather than dozens or hundreds of floppy disks.

There are many different kinds of tape drives: internal, external, and in many dif-

NEWS

fore
lost,
that

your
n be
rson
r for
and

d by
your
vent
the

Back up your data and lock up you

■ PROTECTION

ferent sizes. Many companies make tape drives, and they range in price from below $200 to over $1,000 for fancier (and more reliable) models. If you're buying a new machine, consider getting a built-in tape drive.

Some tape drives for IBM-compatible machines run off the parallel or printer port. This is especially handy if you have a laptop computer or more than one machine. The Colorado Trakker models are among several such tape drives.

Even if you can get everything on a single tape, you need more than one. Users should rotate their backups between several tapes. For example, you might have four tapes, using each tape to do a complete backup once a week. At the end of the fifth week, simply reuse the first backup tape.

It is also a good idea to make archival backups every three to six months. These should be put away for your long-term archives.

Once you make a backup, Spafford says, it's important to test the tapes or disks from time to time to make sure that the information is there. Some backup software backs up data to a floppy disk or a tape but doesn't routinely verify that the backed-up data has really been backed-up; doing so doubles the time that the backup requires.

You can choose from many backup software programs almost regardless of what kind of computer you use. Retrospect, a popular backup program for Macintosh computers made by Dantz, can be set up to schedule backups on a regular basis.

On the PC side there are many popular backup utilities, including the ones that come with the MS-DOS and PC DOS operating systems. A popular add-on package is Norton Backup, by Symantec.

Many computer users don't bother to back up their application programs, since application programs are usually quite large and legal users already have a copy of the software on the original distribution disks. Unfortunately, this strategy is short-sighted in many cases. That's because many programs have complicated configuration files and preference databases that are customized for the user after the software is installed. Unless the entire program is backed up, it can take many hours, or even many days, to reinstall and recon-

Make sure you protect your computer from viruses

One important way to protect data is to make sure your computer is protected from viruses. These are software programs that can corrupt your vital files and make the data unusable. They don't hit very often, but when they do they can be very bad news.

You can get software viruses from many sources. The most common is an infected diskette that you put into your computer, which then picks up the infection. A less common way is to download an infected file from a bulletin board, commercial on-line service or the Internet.

Many companies sell virus-protection software. You may already have some, if you own recent versions of Microsoft's MS-DOS or IBM's PC DOS for IBM-compatible computers.

Retailers also sell virus-protection software. Read the directions carefully before you use it, but use it.

Look for an upcoming article on viruses and virus-protection in the Computing section.

From backups to encryption to plain old common sense, you can lessen the chances of losing your data or your machine, security experts say.

---

figure all of the software from the distribution disks.

Spafford also recommends that home users make a copy of their distribution disks — the diskettes in the software package itself — before trying to install new software. The copies protect the user in case something goes wrong with the installation, and are useful backups in the event that the original distribution disks are lost.

"For large-scale installations, the vendors will provide copies of software if you are a registered user," he notes. "But for home use they won't do it without a charge."

You don't necessarily need a tape drive to back up your computer. Several companies, including Iomega and SyQuest, sell removable drives that work like external hard disks.

One of these, Iomega's new Zip Drive, costs about $200. It stores 100 megabytes on a proprietary 3.5-inch cartridge that acts like an additional hard drive and costs about $20. Although using a Zip Drive and other removable drives can be much more expensive than using a conventional tape system, it is much faster and easier to retrieve specific files from your backup.

Your data will also disappear if you lose your computer. In my neighborhood, there has been a

rise in the number of laptop thefts out of residences. Laptop computers are expensive and easily resold. Desktop computers are also frequently the targets of theft.

But a few simple measures can dramatically reduce the chances that your computer will be stolen. The simplest: Lock your computer down with a chain or cable.

Desktop computers can be secured relatively easily. Many computer stores sell a product that consists of a cable and hooks, mounted to your computer and monitor (and even the keyboard) with high-strength glue; you thread the cable through the hooks and wrap it around a radiator or some other securely fastened object.

If you don't want to mark up your computer desk, another alternative is etching your name, address and phone number onto the computer's case with an engraving tool. Many police departments will lend you such a tool for overnight use; while you have it, you might want to etch your name in your stereo and television set as well.

Laptop security brings its own set of problems. In my office, I had a Toshiba 3100 portable computer with a chain around its screen and fastened to a nearby radiator with a pair of padlocks. When I traveled, I would lock the computer to the desk in my hotel room. The only problem with the

lock up your computer

›u protect
r from viruses

from a bulletin board, commercial on-line service or the Internet.

Many companies sell virus-protection software. You may already have some, if you own recent versions of Microsoft's MS-DOS or IBM's PC DOS for IBM-compatible computers.

Retailers also sell virus-protection software. Read the directions carefully before you use it, but use it.

Look for an upcoming article on viruses and virus-protection in the Computing section.

---

n to plain old common sense,

) of losing your data or your

›ey.

rise in the number of laptop thefts out of residences. Laptop computers are expensive and easily resold. Desktop computers are also frequently the targets of theft.

But a few simple measures can dramatically reduce the chances that your computer will be stolen. The simplest: Lock your computer down with a chain or cable.

Desktop computers can be secured relatively easily. Many computer stores sell a product that consists of a cable and hooks, mounted to your computer and monitor (and even the keyboard) with high-strength glue; you thread the cable through the hooks and wrap it around a radiator or some other securely fastened object.

If you don't want to mark up your computer desk, another alternative is etching your name, address and phone number onto the computer's case with an engraving tool. Many police departments will lend you such a tool for overnight use; while you have it, you might want to etch your name in your stereo and television set as well.

Laptop security brings its own set of problems. In my office, I had a Toshiba 3100 portable computer with a chain around its screen and fastened to a nearby radiator with a pair of padlocks. When I traveled, I would lock the computer to the desk in my hotel room. The only problem with the

security system was its weight: about 5 pounds, including the chain and the locks, on top of the weight of the machine itself.

Things are much easier, or at least lighter, now. Kensington Microware Limited has a 5.5-ounce security system that works with a variety of laptop computers including Apple's PowerBooks, IBM's ThinkPads, and computers made by AST, Compaq, Dell, Digital, Toshiba and others. The cable has a loop at one end which can be secured to a desk or a radiator, and a lock at the other end that attaches to the special security slot that is built into many laptops.

No matter what you do to keep your computer secure, a determined thief probably can steal it. Make sure you're covered by theft and accident insurance; your homeowner's policy may not cover the entire value of your gear, so you may need a supplemental policy, especially if you use your computer for business.

If you use your computer for paying your bills, keeping track of your personal finances, or simply storing confidential information, then the possibility of theft should give you extra reason to worry; not only will the thief have your valuable computer, but he or she will potentially have all of your financial information as well. Frequently, this might be worth many times the value of the computer itself.

One thing that you can do to minimize the threat of theft is to use encryption.

Encryption is a technique for scrambling information so that it cannot be read by people who are not authorized. With most encryption systems, you type a password or a pass phrase to encrypt your data; when you want to read your data back, you type the same password to unlock the information.

There are many different encryption systems available for personal computers. Utility software from Symantec and other companies may be enough for you.

An increasingly popular system is PGP, Pretty Good Privacy, by Phil Zimmermann. PGP is available for free over the Internet and major on-line services for non-commercial use, and can be purchased from Viacrypt (Phoenix, Ariz.). Besides encrypting files, you can also use PGP to encrypt electronic mail that you are sending to someone else.

Simson Garfinkel's latest book is "PGP: Pretty Good Privacy," published by O'Reilly & Associates Inc.

Visual Bas programn

BY GREG KANE
Knight-Ridder News Service

When Mark Allen upgraded the projection system his company used to stage corporate meetings, he discovered he needed to create a computer program to control a $60,000 projector whose standard controls flash on the main screen. "That would ruin the whole event," says Allen.

With programming experience limited to long ago introductory courses in BASIC and Pascal, Allen toyed with programming a palm-top ("Talk about reminiscences of Pascal," he shudders), hefted a C++ primer (deciding, "Man this is going to take forever") and finally ended up doing what thousands of other business have done, buying a copy of Visual Basic for Windows.

He didn't buy a package that makes programming a Mac truly easy, because there isn't one. Mac programs are controlled by a Rube Goldberg maze of ifs and do-whiles that programmers must construct from scratch for each program they write. Programming a Mac, like cooking on a wood stove, is harder than it needs to be.

Windows is different. Just as early Macs let non-hackers use computers, Visual Basic (version 3.0, street price $100, Microsoft, (800) 426-9400) lets inexperienced programmers make powerful Windows software.

Visual Basic programs are quick to construct and easy to modify because Visual Basic takes full responsibility for all the button, menu and window manipulation routines at the center of every program.

A Visual Basic programmer's only responsibility to the Windows interface is to draw the menus, buttons and other