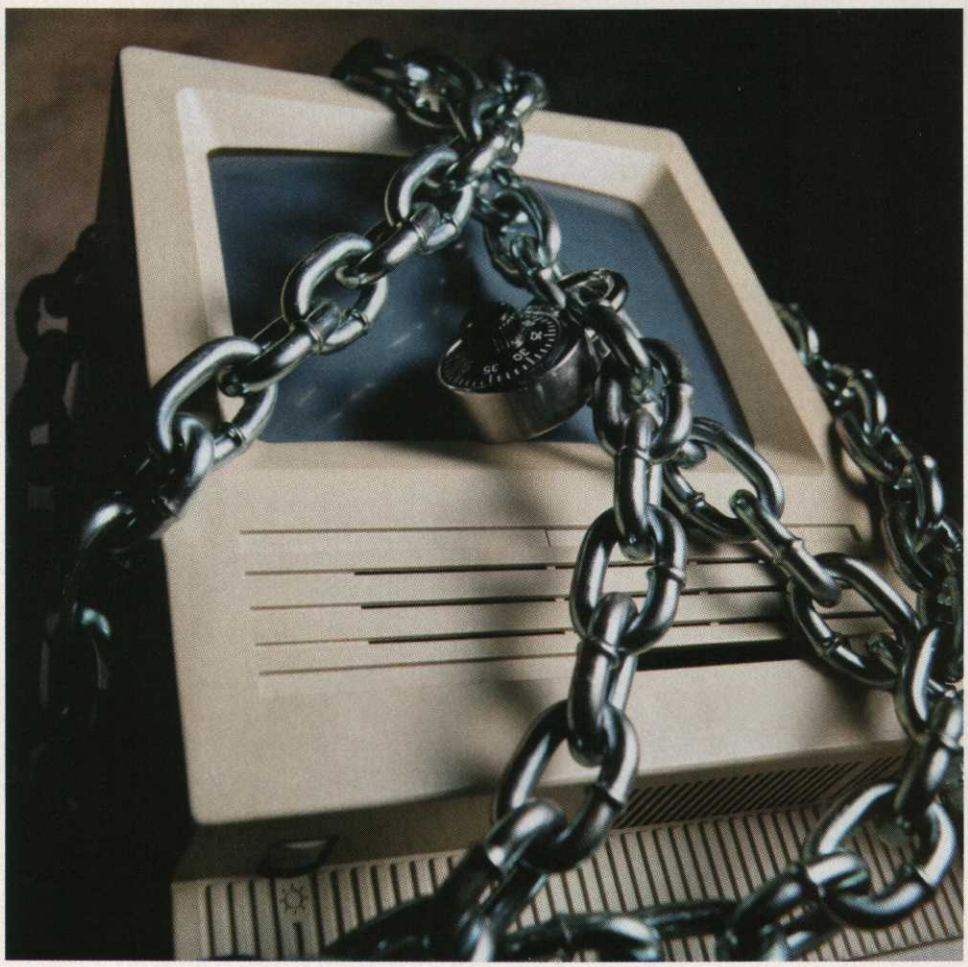
Data Defense

Since computers now hold much of your vital business information, what are YOU doing to protect it?

BY PETER L. MCCORMICK

As personal computers have taken on increasingly significant roles in our personal and professional lives, security has become a concern for all of us — because sooner or later the computer gremlins are going to get you.

Think of computer security as preventing the loss of valuable data. While your computer and the software on it can be replaced, the important stuff — your correspondence, reports, databases, spreadsheets and other data files — often can't. Let's look at the most common causes of data loss and the steps you can take to prevent it.



PHOTODISC

The crash

A computer crash is anything that causes your computer to stop working. Computer crashes can result from overloading an undersized hard disc, conflicts associated with new software installations or upgrades, computer viruses and even mechanical malfunctions within the computer itself.

The first line of defense against any computer crash is the data backup, which simply means saving your files somewhere else. It doesn't matter where you save them as long as you save them regularly. You should do it at least weekly, if not daily, depending on how frequently your data changes.

Automated utilities like

AutoSave, DriveImage, NovaBackup, Norton Ghost or Retrospect Desktop Backup can do a file-by-file backup of your entire hard drive. Either way, having your data files stored in one directory or folder simplifies the backup process.

The My Documents folder within the Windows 95/98/2000 operating systems is a ready-made starting point. Create an underlying directory structure within My Documents and store your data files there. Back up that one folder, and your data is safe — well, almost.

While backing up files on a removable media is good, most often that tape, Zip disc or CD is left sitting in the drive bay until the next backup. What happens if your computer is stolen, fried by lightning or destroyed by fire? Poof — your data and the backup go with it.

To protect against physical loss, the new breed of remote online backup services (such as *Skydesk.com*, *StoragePoint.com*, *Driveway.com* or *Visto.com*) create scheduled backups and securely transmit your data over the Internet to a remote storage site (for free or a small fee). In the event of a data loss, simply log in to that site and retrieve your backup files.

A utility like PowerQuest's SecondChance takes periodic snapshots (called checkpoints) of your hard disc and system configuration. When a hardware or software gremlin rears its head, simply load a previous snapshot and your computer is restored to its preglitch state.

Since most backup systems compress files into smaller copies of the original, none is foolproof. Test the backup process to ensure that you can successfully recover data from those files when needed.

Lightning is the most common cause of mechanical failure of computers on golf courses. Buy the best universal power supply unit you can find, or consider a commercial surge protection system for your entire home, office or maintenance building. The $300 to $1,500 investment in lightning and surge protection is worth it.

Virus protection

Computer viruses have made anti-virus software a critical defense against unwanted intruders. Viruses are infectious files created by those who delight in causing problems for others. While the Internet has made sharing files fast and easy, it has also allowed viruses to proliferate via e-mail, file attachments and software downloads.

Use virus detection software (Norton AntiVirus and McAfee ViruScan are industry standards) to scan your hard disc, all portable storage discs, as well as incoming e-mail and file attachments — and then either clean or delete all infected files. Since new viruses appear constantly, subscribe to the updating service (usually $20 to $30 annually) offered by your anti-virus software provider. This will keep your virus detection database aware of the current viruses that are circulating.

Since many viruses are hidden in executable (.exe) files or within macros in Microsoft Word (.doc) files, a good rule is to not open any .exe or .doc file attachments you receive from unknown sources.

In the case of the Pretty Park virus that circulated this spring, even known sources weren't safe. If you received the Pretty Park virus, it arrived in a message from someone who had your e-mail address in an address book. While not destructive, the virus would establish itself in your system and then send itself to everyone in your e-mail address book. To be safe, scan every e-mail attachment you receive for viruses, regardless of the source.

Don't get hacked

A computer hacker need not be a propeller-headed techno-nerd holed up in a computer lab somewhere. It could just as easily be the little old lady down the street.

If you use one of the new always-on high-speed Internet connections such as cable or digital subscriber line services, you may be leaving yourself open to snooping.

All computers hooked into these services are on a giant network with fixed numerical Internet addresses, so it's relatively easy for anyone so inclined to explore your computer unless you have precautions in place. You are much less at risk if you connect to the Internet via a dial-up service, since your service provider assigns a random IP address each time you connect.

Networking computers in the home or office to share printers, files or Internet access opens further opportunities for unwelcome visitors to your system. For a single computer connected to a cable or DSL Internet connection, make sure "file sharing" is turned off in your operating system preferences.

Lightning is the most common cause of mechanical failure of computers on golf courses.

For further protection against intruders (and highly recommended for a networked environment where file sharing is usually enabled), a personal firewall program like Norton Internet Security 2000, BlackICE Defender or ConSeal Private Desktop give you sophisticated privacy features to block unauthorized communications to or from your personal computer or network.

One last suggestion: The next time you clean your office, gather up all those software CDs and jewel cases with the product ID codes on the back and organize them in one place. Should your computer fail beyond recovery and you must start fresh with a new hard disc before restoring your backup files, having those program CDs and product IDs handy will greatly speed the process. ■

Peter L. McCormick is president, editor and webmaster of TurfNet Associates in Skillman, NJ.