Psychiatric Bulletin (1992), **16**, 771–773

Computers in psychiatry

2. Viruses – prevention, detection, and removal

BANKOLE A. JOHNSON, Wellcome Research Fellow, University of Oxford Department of Psychiatry, Psychopharmacology Research Unit, Littlemore Hospital, Littlemore, Oxford OX4 4XN; E-mail: Kole @ U.K. AC. Oxford. Vax; and LYNDA T. WELLS, Registrar, Nuffield Department of Anaesthetics, John Radcliffe Hospital, Oxford OX3 9DU

Most medical researchers rely on computers to store their data, often many years of work. It is, however, surprising that many give little thought to protecting their machine from malicious damage caused by computer viruses. This article examines how to prevent, detect, and remove computer viruses.

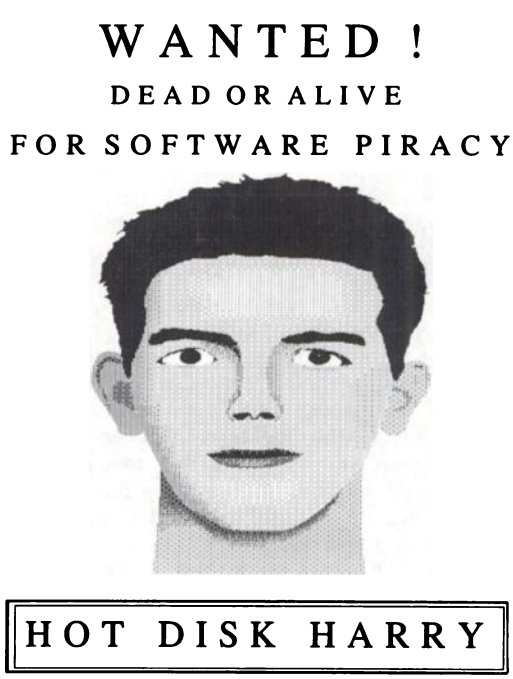
What is a virus?

Viruses are small pieces of code hidden within legitimate computer programmes. They are intentionally written and disseminated to damage other programmes (software) or data files, erase part or all of the hard disk, or impair computer performance. They, however, do not damage the computer's hardware. Like biological viruses, they infect other applications and make copies of themselves. Some, like the *Michelangelo* virus, are configured to become active on or from a certain date. Viral infections are on the increase. In Britain, the Computer Crime Unit of the Metropolitan Police collates information and provides warning of outbreaks.

The different types of virus

Viruses are of two main types: (a) those that infect a special part of floppy or hard disks, the boot sector – which loads the Disk Operating System (DOS) – or the partition table of a hard disk and (b) file viruses which copy themselves onto executable files; on International Business Machine (IBM) compatibles, these files have .com, .exe, .sys, or .ovl extensions.

Boot sector viruses copy themselves from infected floppy disks into the computer's memory when the machine is started, and replace the hard disk's normal boot sector. A common boot sector virus, "stoned", displays the message *"your computer is now stoned"*. All formatted floppy disks contain boot sectors. This is not the same as a **bootable disk:** a formatted disk which contains all the special programmes (system files) needed to start the computer. If you have not already taken the precaution of making a bootable disk, which can be used to restart the computer if the hard disk fails (crashes), insert an unformatted floppy disk into your machine, and at the [X]:\> prompt *type* FORMAT [Y]: /S and press *enter;* [X] denotes the hard and [Y] the floppy disk drive.



File viruses can be transferred from infected programmes on floppy disks, networks, or Bulletin Board Services (BBS). Data files carry no risk of infection but can be damaged by viruses.

Trojan horse programmes like viruses impair computer performance; in contrast, they are unable to copy themselves to other applications and can damage hardware. They are often hidden within a useful utility or game package and become active on or from a predetermined date.

Common-sense precautions: prevention is better than cure

- You are responsible for the information on your computer. Do not allow access to your computer on demand, even to friends. Information on shared computers must also be owned and looked after by a designated person; other users should be persuaded, diplomatically, to agree to a code of practice which provides security without unnecessary inconvenience.
- Do not accept pirated software. It is illegal and the commonest method of acquiring a virus. Do not use "free" promotional disks. A couple of years ago, many people were mailed "free" anti-virus software; it contained the *Aids* computer virus!
- Before use, always check floppy disks for viruses by scanning with an anti-virus programme (see below).
- Download programmes from BBS or networks onto a floppy disk. Then, scan the disk for viruses.
- Do not boot from a floppy disk, or with one in the floppy disk drive.
- Write-protect your bootable disk and as many of your other disks as is practicable; viruses cannot infect write-protected disks.
- Buy software from a reputable dealer. Before installation, write-protect and backup the original disks.
- If you know the date a virus will become active reset your computer's clock. Because some viruses are initialised from, rather than on a particular date backdating may be more fail-safe than advancing the clock.
- Take regular backups, at least weekly. It is your only insurance policy against hard disk failure. Keep a backup log, stick to a rigid routine, and organise the disks you intend to use on a cyclical rotation.

  Incremental backups are less time-consuming because only files and subdirectories that have changed since the last copy was taken are duplicated. A useful tip is to use the Disk Operating System (DOS) XCOPY rather than the BACKUP command. For example, at the [X]:\> prompt type XCOPY [X]:*.* [Y]: /S /M – where [X] denotes the hard and [Y] the floppy disk drive. When [Y] is full, insert a new disk and repeat the command; those files and sub directories already copied will not be duplicated on the next disk.
- Ensure, using a virus scanner, that you are not backing up infected copies of your data or programmes. Keep backups at a different site in a locked fireproof box.

Anti-virus software

Anti-virus packages prevent, detect and remove computer viruses. None offers total security. Choose one which suits the way you work.

Prevention

Some anti-virus packages use Terminate and Stay Resident (TSR) programmes to prevent viruses from loading into the computer's memory. Packages which use TSRs must be chosen carefully because they can conflict with other memory resident programmes.

Detection

Scanners work in two ways. They can: (a) check each file on a disk for a code (signature) belonging to a particular virus or (b) assign a specific algorithm (fingerprint or checksum) to all executable files, the partition table, and the boot sector. A list of these checksums is compiled and stored on the hard disk. When the scanner is initialised, it compares the checksums generated with the ones on record. Mismatches give rise to warnings. An antivirus programme which allows files on which checksums are performed to be specified and updated is essential; otherwise, false alarms will occur as a result of intentional changes to the system's configuration. Programmes which metamorphose on execution such as compilers may also cause false alarms. If used properly, and updated regularly, a good scanner will detect most known viruses. Examples include Sophos anti-virus software and McAfee's viruscan.

Removal

Programmes such as Central Point anti-virus or Norton's anti-virus disinfect contaminated files by removing the viruses's signature code. As an added precaution these files should be deleted and restored from the original programme or uninfected backup disks.

What if disaster strikes?

If your computer starts to behave erratically – for example, the letters on the display fall to the bottom of the screen, or strange messages are displayed – it may be infected with a virus.

- Do not panic.
- Save your work and switch off the machine.
- Use your write-protected bootable disk to restart the computer. This ensures that no more viruses are left in memory to contaminate other files.

https://doi.org/10.1192/pb.16.12.771 Published online by Cambridge University Press

- Scan your hard disk, including all logical and network drives, with an anti-virus programme. Infected files should, ideally, be deleted and reinstalled from clean backups. If deletion is not practical, an appropriate anti-virus package can be used to repair contaminated files. After a successful repair or deletion, re-scan the hard disk to confirm it is clean.
- Scan all floppy disks and backup files to locate the source of the infection. throw the infected disk away.
- Notify your colleagues – so they can check their computers and floppy disks.
- Report the incident to the Computer Crime Unit.
- If the virus cannot be removed by these simple measures, or you are a complete novice at computing or in any doubt about the best thing to do, do not dabble. Get expert help. Try your local University's computer advisory service. If this service is not available to you, advice can be obtained from Virus News International (S & S International, Berkley Court, Herts HP4 2HB, Telephone 0422 877877).
- If all attempts to remove the virus fail the hard disk will have to be re-formatted. The software will have to be re-installed and your data recreated from backup disks. Avoid disaster: take regular backups!

In summary, prevention is better than cure. Infection by computer viruses can be avoided by ownership of information and good computing techniques. While anti-virus software can assist with recovery from a viral infection, it is critical to perform regular backups.

Further reading

SOMESON, P. (1991) *DOS Power Tools – Techniques, Tricks and Utilities*. Toronto: Bantam Books.

Psychiatric Bulletin (1992), **16**, 773–775

Innovations

An integrated service for mentally disordered offenders

SUBE BANERJEE, Research Fellow, UMDS (Guy's Campus) & The Health Care Centre, HMP Belmarsh, Western Way, Thamesmead, London SE28 0EB; TIM EXWORTHY, Research Fellow, UMDS (Guy's Campus) & South East London Court Liaison Scheme; KIKI O'NEILL-BYRNE, Research Fellow, UMDS (Guy's Campus) & HMP Belmarsh; and JANET PARROTT, Consultant Forensic Psychiatrist, Bracton Clinic, Bexley Hospital & HMP Belmarsh

In recent years there has been increasing concern about the plight of the mentally ill in prisons, particularly those on remand. The 1976 Bail Act gives everyone the right to unconditional bail but mentally disordered offenders find themselves disadvantaged in that their right to bail can be set aside not only because of the gravity of the alleged offence but also for reasons consequent to their mental illness. These include lack of community ties, their own protection or most commonly for the preparation of psychiatric reports. The mentally disordered may thus be remanded in custody even if the charge against them is minor or not punishable by imprisonment.

Coid (1988) and Bowden (1978) have drawn attention to the fact that at the end of a period of remand

https://doi.org/10.1192/pb.16.12.771 Published online by Cambridge University Press