

Sophos - Simple steps to defend against viruses, spyware and adware

Use anti-virus software

Install anti-virus software on all of your desktops and servers, and ensure they are kept up to date. Because new viruses can spread extremely quickly, it is important to have an updating infrastructure in place which can update all the computers in your company seamlessly, frequently, and at short notice. Sophos's anti-virus solutions can be automatically updated, ensuring the latest virus and spyware protection is in place against the latest threats even when your office is unmanned.

Run a consolidated email filtering solution at your email gateway as well to protect your business from the threats of email-borne viruses, spam and spyware. Sophos email security checks all email traffic passing through your email server, providing an extra layer of protection against mass-mailing worms and viruses at the gateway.

And don't forget to protect your laptop computers and desktop computers used by home workers. Ensure they are running up-to-date virus protection as viruses, worms and spyware can easily use these devices to enter your business. Sophos can easily ensure that your laptop and remote workforce are automatically updated with the latest virus protection every time they connect to the internet or your network.

Set your filtering

Consider filtering potentially malicious emails at the email gateway as this can provide a level of pro-active protection against new threats.

You could:

- **Block file types that are often virus carriers**
These include EXE, COM, PIF, SCR, VBS, SHS, CHM and BAT file types. It is unlikely that your organization will ever need to receive files of these types from the outside world.
- **Block any file with more than one file type extension**
Some viruses attempt to disguise their true executable nature by using "double extensions". Files such as LOVE-LETTER-FOR-YOU.TXT.VBS or ANNAKOURNIKOVA.JPG.VBS may appear to be ASCII text or a harmless graphic to the inexperienced.
- **Ensure all executable code sent to your organization is checked and approved**
Ensure that all executables received from the outside world via email goes directly to your IT department or, in the case of small businesses, your IT person, for checking and approval.

This serves two purposes. First, your IT department (or person) can confirm not only that it is virus-free, but also properly licensed, unlikely to conflict with existing software applications, and is suitable (for instance, not pornographic). Second, IT will always know what software is installed on which computers.

Stay informed about the latest virus threats

Subscribe to Sophos's mailing lists for up-to-date information on the latest virus threats, support information, and new product developments. At the same time, consider adding a live virus information feed to your website or intranet to ensure your users know about the very latest computer viruses.

Protect the gateway and remote users with firewalls

Computers connected to the outside world should be properly protected from internet threats via firewalls. Laptops and remote home workers should be included; they will also need firewall protection and might not be able to take advantage of a central firewall inside your business.

Stay up-to-date with software patches

Many software vendors issue advisories on security issues. For instance, Microsoft runs a mailing list which warns of security loopholes and issues found in Microsoft's software and advises on patches which are available for protection. IT should subscribe to such mailing lists, and act upon the advisories as appropriate. When a new security hole is found in an application or operating system, and a patch is available, organizations should have an infrastructure for testing the patch works properly and rolling that patch out across their userbase. Some vendors may provide automatic patch updating for home users, and such systems may be appropriate for updating your mobile workforce and remote homeworkers with the latest security fixes.

Back up your data regularly

Make regular backups of important work and data, and check that the backups were successful. You should also find a safe place to store your back-ups, perhaps even off-site in case of fire.

Disable booting from floppy disks

Although they are not as commonly encountered as they used to be, boot sector viruses can still affect computers and yet can be easily countered. Change the CMOS bootup sequence on PCs so that rather than booting from drive A: if you leave a floppy in your machine, you boot by default from drive C: instead. This should stop all pure boot sector viruses (like Form, CMOS4, AntiCMOS, Monkey, etc) from infecting you. Should you need to boot from a floppy disk the CMOS can easily be switched back.

Introduce an anti-virus policy

Produce a policy for safe computing and distribute it to all staff. Make sure every employee has read and understood the policy, and that they know who to speak to, if they have any questions.

Such a policy could include:

- A ban on downloading executables and documents directly from the internet.
- A ban on running unsolicited executables/documents/spreadsheets within the organisation.
- A ban on playing computer games or using screensavers which did not come with the operating system.
- An IT checking and approval system for executables that arrive via email from the outside world.

It could also ask staff to do the following:

- Save all Word documents as RTF (Rich Text Format) files as DOC files can harbour macro viruses.
- Treat with suspicion any newly arrived email that they weren't expecting.
- Forward any virus warnings or hoaxes directly to IT (and no-one else) to confirm whether they are genuine or not.
- Staff should inform IT immediately if they think their computer has been infected with a virus.