

## **INFORMATION SECURITY: HOW TO PROTECT YOURSELF AGAINST COMPUTER VIRUSES**

[What is a virus?](#)

[How do I know if a virus has infected my system?](#)

[Prevention](#)

[Virus defence software](#)

[Alert services](#)

[Recovery](#)

[Summary](#)

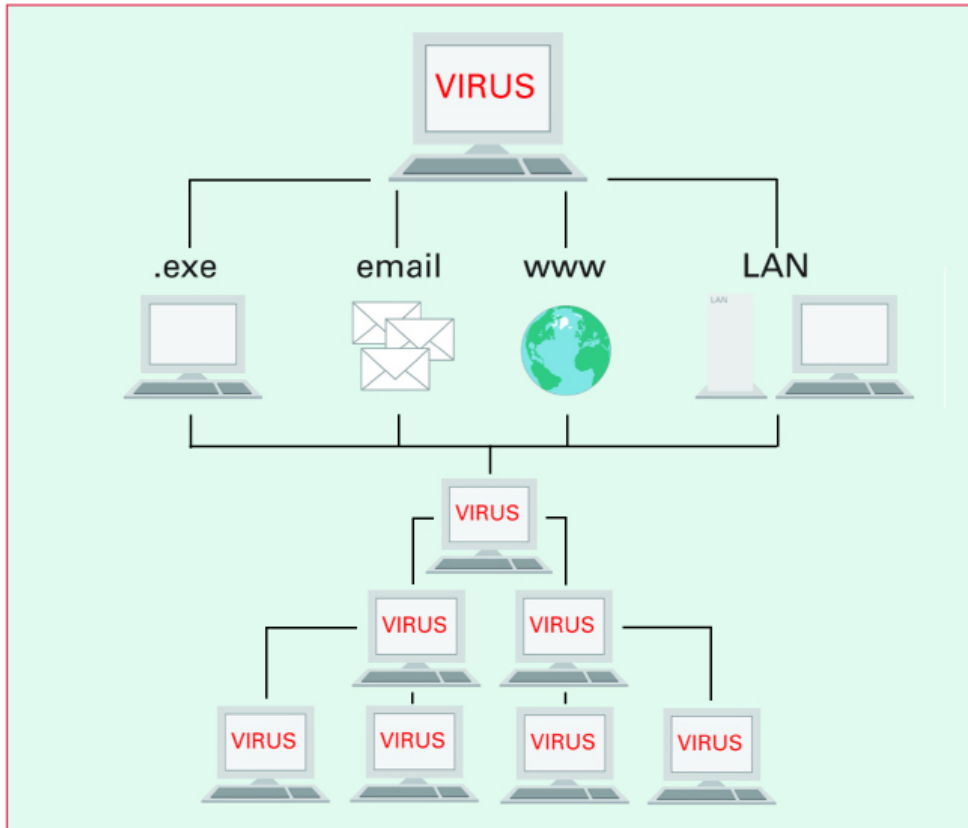
[Further help and advice](#)

### **What is a virus?**

A virus is a computer programme that is designed to spread from machine to machine and from network to network, while performing some operation on the infected systems. Many are harmless but others can be very destructive. For example, some viruses can totally stall an organisation's computer systems. Some of the best-known viruses include:

- Love Bug
- Melissa
- Bubbleboy
- Code Red
- Nimda.

Viruses normally spread via e-mail (in attached files) by web browsers and by sharing files on discs and CDs (see the diagram below). Some are self-contained programmes, while others are planted into standard applications (such as Microsoft Word and Excel) and 'piggyback' parts of their functionality.



Usually, viruses fall into the following categories:

- macro viruses which 'piggyback' features within standard applications such as Microsoft Word and Excel
- e-mail viruses which are the most commonly distributed viruses and can infect systems without user intervention
- HTML viruses which cause infection while users visit certain Internet pages
- file viruses which are normally attached to files transferred by disc, CD, file transfer or are attached as files to e-mails
- morphing viruses which are able to modify their form to avoid detection. They can even change the method by which they cause damage
- stealth viruses which are able to hide themselves by separating their component parts or by scrambling (encrypting) their codes.

A virus can cause your system to behave in a number of ways ranging from the annoying (e.g. the playing of a tune) to the destructive (e.g. the removal of files or making unrecoverable changes to them). Some viruses remain hidden and change data gradually to avoid detection (until, of course, it's too late).

### **How do I know if a virus has infected my system?**

There are some basic signs to look out for. Some are very obvious (certain viruses actually tell you they've infected your machine). Remember that the following signs will often have other causes; they are not definitive proof of infection.

- Your system slows down. This can be especially noticeable if your machine is connected to a network.

- You see activity on your machine that you think you did not cause. For example, a disc drive light may come on unexpectedly.
- If you are running an internal e-mail server, you find that this becomes overloaded and slows down.
- Your data files become corrupted or go missing. Sometimes, regular programmes such as Microsoft Word or Excel will respond with a message telling you that the file you're trying to load is not in the correct format.
- There is an unexpected change in the content of your files.

### **Prevention**

The risk of virus infection can be minimised by a combination of common sense, vigilance, virus defence software and the use of virus alert services. The most effective solutions use a combination of these. The following sections describe some general steps to take to prevent a virus infection.

#### Common sense and vigilance

- Keep your premises physically secure. This makes good sense in all circumstances, especially as some intruders have been known to introduce viruses deliberately by using infected floppy discs.
- Do not open suspicious e-mails or attachments. Treat as suspicious any e-mails from:
  - anonymous senders
  - strangers addressing you in a familiar manner
  - non-standard addresses.

One simple way to check is to telephone the alleged sender (if possible) to confirm their ID and credentials.

- Be especially wary of any messages that match the types listed above and contain attachments with the .EXE, .SCR or .VBS file extension names.

Remember that viruses can also lurk in more familiar files, such as Microsoft Word and Excel attachments. These can contain macro viruses.

- Beware of hoax virus alerts. Think twice before forwarding virus-warning messages, especially if they have come from an informal source. These hoax messages can spread just as fast and as far as viruses and cause as many problems.
- Never forward any comedy or joke programmes to anyone via e-mail. If you must share a joke, send the Internet link and not the programme file itself.
- If you are unsure, you can save suspicious attachments to your local directory then use virus defence software to examine them in more detail.

### **Virus defence software**

Basic actions (again, based on common sense) should include the following:

- Keep your Internet browser up-to-date by 'patching' it regularly. Most browser updates include new security elements to meet newly identified virus threats. These updates can be obtained from Microsoft (for Internet Explorer) or Netscape.
- Purchase virus defence software. You should identify your individual requirements depending on your technical infrastructure, geographic spread and dependency on technology.

- Suppliers offer many kinds of anti-virus programmes, some of which are downloadable from their web sites.
- Use this software to scan e-mail attachments for viruses before you open them and also run an anti-virus programme that scans files as they are opened. This type of scanning should take place constantly, automatically checking every file, programme, or document each time it is opened or used.

Any technical solutions need to be managed. The following steps provide a simple framework.

- Define a virus defence strategy, addressing:
  - gateway virus checking
  - server virus checks
  - workstation virus checks
  - update mechanism for patches and fixes
  - isolation policy
  - recovery procedures.

### **Alert services**

Virus alert services are provided by a number of bodies, including:

European Institute for Computer Anti-Virus Research

[www.eicar.org](http://www.eicar.org)

Symantec Security Response

[http://www.symantec.com/en/uk/business/security\\_response/index.jsp](http://www.symantec.com/en/uk/business/security_response/index.jsp)

Sophos Virus Information

<http://www.sophos.com/security/>

F-Secure Security Information Centre

[http://www.f-secure.com/security\\_center/](http://www.f-secure.com/security_center/)

Computer Security Resource Centre Virus Information

<http://nvd.nist.gov/>

Virus Bulletin: Independent Anti-Virus Advice

[www.virusbtn.com](http://www.virusbtn.com)

Details on subscription to these services can be obtained directly from the service itself. If alerts are used, they should be combined with a practical procedure for updating the systems at risk, including your servers, desktops and laptops.

N.B. Inclusion of companies listed on these pages does not reflect any form of endorsement by BERR. Links are detailed because sites may provide virus alerting services that you may find useful. This is by no means a definitive list and you are advised to research any company and products carefully prior to purchasing goods or services.

### **Recovery**

A virus infection can have a massive effect on your business. Past infections (including the notorious 'NIMDA', 'I Love You' and 'Code Red' viruses) have cost many millions of pounds to manage.

If you do use virus defence software and your system becomes infected, call your software supplier. The major suppliers act as information clearing houses during virus outbreaks and have details about many variants of the thousands of viruses that exist. They also have extensive research information on possible future viruses.

You may wish to inform regular contacts (suppliers, partners etc.) if you suspect you have sent them a virus. Follow these initial steps to start the recovery process.

Step 1: Tell everyone who needs to know

If the virus is spread through e-mail, tell everyone who has an e-mail account on the infected system about it as quickly as you can. Better still, use whatever means you have to prevent the unwanted email coming into your system altogether.

If there is a specific file attachment that contains the malicious virus programme, name it and threaten anyone who opens it thereafter with drastic action. There are many methods of letting people know about the problem such as:

- putting up warning posters at all entrances and exits to company offices
- sending out SMS messages to staff mobile phones. These methods are especially useful if the initial attack has happened overnight, as users may open the malicious e-mail before they have seen any warning sent by e-mail.

Step 2: Eradicate the virus

You can often download free fixes and patches from the Internet. Make sure your software is up-to date before starting the eradication process and keep the following points in mind:

- When attempting to remove a virus always ensure that your virus scanner is updated using the latest pattern files. Failure to do so may result in damage to your data.
- Close all applications and disconnect affected computers from all networks. You should also disconnect any modems or external connections.
- Use your virus defence software to scan all hard discs on the affected computers and files. Examine any resulting report carefully.
- Never reconnect affected machines until they are confirmed to be 100% virus-free.
- Scan any floppy discs that may have been in contact with the affected machines.
- Tell anyone that you think may have been infected and advise them of the necessary steps to take to remove the virus.
- Make use of your virus defence software supplier. They can supply direct services to assist you and help to make sure your own actions are appropriate.

Step 3: Organise a clean-up operation

- Plan a systematic sweep of all affected machines; sometimes you have to clean every machine, even if it has not displayed any signs of infection.
- Contain the spread of the virus by quarantining and disconnect infected machines or systems from the rest of the network.
- If the entire system seems to be infected you may need to disconnect it from any external networks in order to contain the virus.
- Once you are sure the infected systems are quarantined, you need to use the following virus recovery steps:

1. The system administrator should check virus bulletin services from the virus defence software vendors as they often post quick fixes or interim notices. When the

relevant anti-virus fix becomes available, roll it out to all system machines and install it on disconnected machines.

2. If there are no mentions of the virus from any of the virus alert mailing companies it is best practice to send a copy of the virus to your anti-virus vendor. Then if your company was the first to be infected the anti-virus vendor can start work on the fix.

3. Once the fix has been implemented, ensure the virus has not spread to the main servers. Run the anti-virus scanner against each of the servers sequentially, fixing any infected files and ensuring they are clean. This method should systematically clean the entire network of the virus as well as minimising the possibility of infecting the entire system.

Although swift implementation of the quarantine method will still result in the temporary loss of a small part of the network, this is ultimately better than complete loss of a business system.

#### Step 4: Make sure there are no re-infections

Ensure that everyone knows what to do and what not to do. Keep emergency security measures in place until:

- the clean-up is complete
- additional patches are in place to prevent infection.

The system administrator should ensure the business has the latest virus definitions and software patches implemented system-wide. He or she should also install these manually on the infected computers, in an attempt to clean the virus from those machines.

#### Step 5: Manage outgoing e-mail traffic during the crisis

Use whatever facilities you have to prevent malicious programmes being exported through e-mail. You may even consider closing down the outgoing e-mail service.

#### **Summary**

- Most virus infections can be prevented by knowledge and common sense. Make sure you and your staff know the basic rules and treat suspicious files and e-mails appropriately.
- Develop a strategy which anticipates virus threats. This should include software, reporting, recovery and communication.
- Install virus defence software and keep it up-to-date. Remember that it has to be managed. It will become less effective if ignored.
- Keep your Internet browser up-to-date.
- Have a recovery plan and keep lists of relevant telephone numbers, especially your software vendor's.
- If you suffer an infection, tell anyone whom you may have infected. Otherwise there could be substantial adverse PR should they subsequently be affected.

Please refer to the [viruses](#) section in our business advice pages (see below) for further information.

### **Further help and advice**

#### **General**

BERR Information Security Health Check Tool  
<http://www.securityhealthcheck.berr.gov.uk/>

BERR Information Security Home page  
[www.berr.gov.uk/sectors/infosec](http://www.berr.gov.uk/sectors/infosec)

BERR Information Security Business Advice Pages  
<http://www.berr.gov.uk/sectors/infosec/infosecadvice/page10059.html>

BERR Information Security Publications (available to order or download)  
<http://www.berr.gov.uk/sectors/infosec/infosecdownloads/page9935.html>

Published by the Department for Business, Enterprise & Regulatory Reform  
[www.berr.gov.uk](http://www.berr.gov.uk)

© Crown Copyright. URN 09/646.