



Anti-Virus Protection for the University of Greenwich

What is a Virus?

A computer virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user. The term “virus” is also commonly used, albeit erroneously, to refer to many different types of malware and adware programs. A virus can only spread from one computer to another when its host is taken to the uninfected computer, for instance by a user sending it over the internal University network or the external Internet, or by carrying it on a removable medium such as a USB drive. Meanwhile viruses can spread to other computers by infecting files on a network file system or a file system that is accessed by another computer. Viruses are sometimes confused with computer worms and Trojan horses. A worm can spread itself to other computers without needing to be transferred as part of a host, and a Trojan horse is a file that appears harmless. All viruses may cause harm to a computer system’s hosted data, functional performance, or networking throughput, when executed. Some cannot be seen when the program is not running, but as soon as the infected code is run, the virus starts. That is why it is so hard to find viruses and other malware.

Most university computers are connected to the Internet and to local area networks, facilitating the spread of malicious code if not protected.

Are You At Risk?

Some viruses attach themselves to outgoing messages or email themselves to all the people listed in your address book. The sudden flood of email overwhelms mail servers, causing the system to crash. Other viruses are more destructive and may lie dormant until a certain date, then spring to life to do their work. Sometimes a strange message appears on your screen, or data and programs may be modified. In the worst case, all the contents of your hard drive may be wiped out.

What Can You Do About It?

Avoid programs from unknown sources especially the internet, and by only using commercial software, you eliminate almost all of the risk from traditional viruses.

You should make sure that Macro Virus protection is enabled in all Microsoft applications, and you should **NEVER** run macros in a document unless you know what they do.

You should **NEVER** double-click on an email attachment that contains an executable. Attachments that come as Word file **.doc**, spreadsheets **.xls**, images **.jpeg** or **.GIF**, are data files, are non executable and can do no damage. However, you do have to be aware of macro viruses as mentioned above. A file with the extension **exe**, **com**, **vbs**, is an executable, and executable files if harboring a virus, once executed (double-click) will do damage within its programmed remit. A file with the extension **zip** or **rar** can hide other file types, e.g. **.exe**, luring you into false security. Opening one of these attachments may cause an infection.

What We Do

The Office of ILS, on behalf of the university, subscribe to a commercial anti-virus program from McAfee. This is installed on all staff and student computers and is regularly updated to give protection against the latest problems. We have installed scanning software on the main email servers that attempt to detect and quarantine suspected virus-enabled email. They are also setup to check outgoing email for possible infected mail.

We separate networks, give advice but occasionally a virus or a hoax message will get through and appear on your system. These hoax messages cause alarm and confusion and are often 'spoofing attempts' i.e. look as though they come from a legitimate site and ask for your username and password. **DO NOT REPLY TO THESE.**

Hoax Viruses, Spam or Junk Email and Email Chain Letters

Hoax viruses, email spam and email chain letters are all now part of our IT lives. One of the unfortunate by-products of our email culture is the receipt of unwanted emails, often a hoax:

- Telling us about the latest computer 'virus'
- Warning us not to open particular email messages
- Asking us to forward 10 copies of the email to friends (or risk unspecified bad luck)
- Junk emails advertising all sorts of online goodies (usually in bad taste)

Please do not forward these messages on to your colleagues, however worrying the warnings are.

For more information on hoaxes visit:

- <http://www.vmyths.com/hoax.cfm>
- <http://symantec.com/avcenter/hoax.html>
- <http://vil.nai.com/vil/hoaxes.aspx>

Spam or Junk Email

Please, just delete these unwanted emails.

There is very little that can be done about this sort of email abuse. People obtain lists of email addresses in the same way that junk mailers buy address lists or that telephone sales people scan phone directories. Unfortunately, if you use email, your email address becomes 'public property'. Remember, such email is directed at an item on a list – NOT at you personally. The people who send the offensive offers are usually very careful to disguise the source of the emails so it is difficult to track down the original sender and register any complaint.

However, if you are concerned, worried or upset by any unwanted email that you receive please forward it to the Help Desk and we will attempt to take action: helpdesk@gre.ac.uk

Email chain letters

Please do not forward these emails on to your colleagues however appealing, funny or threatening these messages appear to be. The performance of the university's email system will inevitably be affected.