

# Duke Office of Information Technology

## An Important Message for CDSS Customers Regarding Computer Viruses

Please read all of this document. If you do not follow the safety precautions in this document, you may be contributing to the spread of viruses on campus and the Internet as well as compromising your own computer.

Virus files have many variations, so this document does not try to describe every one. The best defense against viruses is practicing "safe computing."

Safe computing at its most basic level includes the following:

- ? Be wary of any email attachment that you were not expecting, whether from a known party or not. Even a friend could send you a virus! If you were not expecting an attachment, contact the sender to confirm the need to open the attachment.
- ? Detach or Save all email attachments to your hard drive, and manually scan them for viruses before opening them. Do not View or Launch attachments directly from email. Doing so will execute whatever virus may be present.
- ? Only download files from the Internet for specific business purposes. If you must download a file, download it to your hard drive and manually scan it before opening.
- ? Do not visit websites that are not for a business purpose. Specifically, don't visit websites that you are encouraged to visit by random ads, chat rooms, Instant Messenger messages from buddies, etc. Such sites could contain a Trojan that could infect your computer.
- ? Ordinarily, just visiting a website without downloading a file should be safe, but hackers occasionally find a vulnerability in the desktop operating system that allows them access to your computer.

NOTE: The virus scanning tools will not protect you from new viruses for which the scanning tools are not prepared. That is why it is critical that you make sure that the attachments are legitimate and that you need them before detaching, scanning and opening them.

Many viruses spread through email by sending bogus messages that say, for example, "Your computer has a virus, click here for details." The "click here" IS the virus. So, do not "click here."

If the virus scanning tool on your computer detects a virus and says it cannot clean it, please unplug the network cable from the computer or shut your computer down. Then call the OIT Service Desk at (919) 684-2200 to report a virus on your computer.

Bogus messages also can be sent using anybody's email address, so that message you receive may not actually be from your supervisor or from Microsoft. That means bogus email also can look like it's coming from you. You might receive messages back from other sites that an email you sent contained a virus. If you have no other reason

to believe your computer has a virus, then that email in all likelihood did not come from you.

OIT's Centralized Device Services and Support group has been configuring all customer PCs to automatically update their virus detection files daily. If you suspect that your virus files may be outdated, please contact the Help Desk at (919) 684-2200.

You can make many other simple changes to your computing configuration and behavior to protect yourselves and your co-workers from viruses, but the four basic steps above will stop the vast majority of the infections.

If you have any questions about working with email attachments or virus scanning, please speak with your local system administrator.

For more information about keeping viruses and other dangerous files out of your work or home computer, visit these sites:

[Virus Protection](#)

[Avoid Online Threats](#)

[Feedback](#)

Duke Office of Information Technology - [www.oit.duke.edu](http://www.oit.duke.edu) - (919) 684-2200 - [help@oit.duke.edu](mailto:help@oit.duke.edu)