

Tip – Identifying Virus Email

Too many email viruses these days are disguised and show up in your Inbox as what looks like a valid email from a colleague at work. This happens when an email virus "spoofs" a valid email address to send a virus as an email attachment.

As soon as an email virus is detected, the CAMail server blocks the infected attachment to stop the infection from reaching the local desktop and laptop computers.

If you receive an email that has garbled text, a strange subject header, etc, please do not open the attachment. By opening the attachment, you are infecting your computer.

In general, please follow these guidelines to safeguard your PC from virus infections:

If you receive a suspicious email:

1. Check the Support Services website for any virus alerts. Alerts are kept up to date as we discover new viruses: http://www.uis.harvard.edu/support_services
2. Delete the message from your Inbox, delete the attachment from C:\Program Files\Qualcomm\Eudora\Attach folder and empty the Trash in Eudora.
3. Never open an attachment, especially an .exe file, unless it is expected.

If you have any questions, please contact the Help Desk at 617-495-8411, or via email to dls@harvard.edu.