

Dear Staff,

We are getting questions about the increasing number of spam emails in people's inboxes. Due to budgetary restraints, we do not now have a spam filter on our email system. Steps can be taken on an individual basis to protect machines from getting viruses, worms and trojans via these emails.

Simple rules to follow to avoid getting viruses via email, and examples of some virus emails.

By keeping these rules in mind, you can avoid the major portion of problems that come through emails.

1. NEVER open an email from someone you do not know. Delete it immediately without opening.
2. Do not open emails that look "odd" or "suspicious." By this, we mean, subjects that are in "bad" English; don't refer to anything that pertains to you; things that might pertain to you, but are from someone who shouldn't have any idea what your email address is; strange, garbled-looking sender names; subjects that are obscene or nearly so, or replace letters with numbers or special characters (an effort to get past spam filters).
3. Virus emails are now being engineered to change sender names and subjects as they spread around. They often have a list of subjects that are designed to be appealing to recipients, or to look like legitimate emails. Use caution with emails you are not expecting.
4. Microsoft NEVER sends patches for its software via emails. Delete these immediately without opening. You must use the Windows Update feature to get patches for your machine.
5. SPS sends only a couple emails from "System Administrator." The only emails SPS sends out from a system account is either a notification that your email box is full (to remedy this problem, just make a note of receiving this email, delete it, and empty out your sent items box, then your deleted items box), or that an email was undeliverable.
6. Many viruses will mail themselves to people you have entered into your address book. If you receive a suspicious email from someone you know, contact that person by phone before opening it and ask if they really sent the email. If they know nothing about it, delete it immediately without opening.
7. Turn off the "Preview Pane" (which shows some or all of an email in your inbox list without having to actually open it first) in Outlook if you use it. Just using that can be enough to become infected by a virus contained in an email. Some emails have embedded graphics in them that will notify the sender that your email address is active, and some will also link to a server to begin downloading a trojan or worm. If you are using the Preview Pane, click on "View" at the top, then click on "Preview Pane" and it will turn it off.

8. Be wary of attachments. Although many can be legitimate, virus emails often use them to spread themselves. Use caution when opening attachments. Do not use a graphical background picture for your emails. It arrives as an attachment and could be manipulated. It also wastes space in email boxes.
9. Keep your AVG up-to-date and make sure it runs a complete scan each day to remove anything you might get.
10. Never make your email address public by entering it on a website somewhere that makes it public – such as on message boards. Always check privacy policies before giving out your email address

Examples of suspicious emails:

1. Emails with or without attachments from “Microsoft.com” with the subject “Install this patch immediately!” or “Use this patch immediately!”
2. Emails with or without attachments from “System Administrator”
3. Emails from “MailNorton@portalpub.com” or from any other address with the following or similar subject “Norton Antivirus detected a violation in a document you authored.”
4. Emails with just “Hi” or “Hello” in the subject line.
5. Emails with the subject “Your recent application is denied”, “Mail transaction failed”, “Test”, “Patch now available”, “Use this patch immediately!” , some tawdry subject, or some other similar subject designed to get your interest.

If you have any further questions regarding email spam, you may contact the Help Desk at 523-HELP.

Thanks to Brian Zahn in the formulation of this document.