



E-mail Address Spoofing

Have you received notices of bounced e-mail messages that you didn't send? Have you received strange, nonsensical, or offensive emails and attachments from what look like a legitimate address? If so, you have probably been the victim of a new recent virus called email spoofing.

"Email Spoofing" means that a message, originally sent from one email account, is actually addressed as if it came from another. While it is almost always possible to know who the actual sender was by looking at the email header, most users do not check this-- they'll only see the "spoofed" email address. Any replies made to the spoofed message, or the notification of an undeliverable message, will be delivered to the spoofed address.

When one of the viruses that use this technique infects a computer, it will search for anything resembling an email address in all personal address books, word processing documents, recently visited websites, and many other types of data. In order to spread itself, the virus will collect all these email addresses in a email containing a copy of the virus, putting one found email address in the 'To:' field, and another in the 'Sender'.

Unfortunately, both the recipient of the email, and the spoofed sender can do very little to avoid having their email addresses used like this. If you have sent an email to someone who is infected with a virus, or if the infected computer has visited a web site containing your email address, you can be a target.

If you post your email address on a website, you should always type out the '@server.com' part— for example, 'at yahoo dot com'. This will make your email address undistinguishable to this virus.

All email received from outside of the College of St. Catherine is scanned for viruses using the most current virus definitions available. As a second layer of protection, all college-owned machines should have McAfee virus scanning software installed.

While you should ALWAYS take care to keep your virus definitions up to date, being the recipient, or even the spoofed sender of an email, does not necessarily mean that you are infected with a virus.