

Re: Mail Bombing, DoS, and Spyware

Source: <http://sci.tech-archive.net/Archive/sci.med.dentistry/2005-01/1062.html>

From: CWatters (*colin.watters_at_pandoraBOX.be*)

Date: 01/10/05

Date: Mon, 10 Jan 2005 08:40:37 GMT

Most of you will know what phishing is all about – see PHISHING below if in doubt – however there is a new twist to watch out for that doesn't rely on you clicking on a link sent by email. It goes like this....

You visit a "harmless" web site that silently installs adware/spyware on your PC. The spyware changes your "hosts file" so that when you try and access PayPal (for example) you are redirected to a fake version without you knowing. Google "what is a hosts file" for more info.

Typically your hosts file lives here on a Windows XP machine.

`c:\windows\system32\drivers\etc\hosts`

You may need administrator access for Windows NT/2000/XP to see it.

DO NOT delete the hosts file as it is usually harmless and sometimes contains information that your ISP needs. Some anti-spyware and pop-up stoppers also change the hosts file.

I would hope that the new MS program prevents programs changing the hosts file without warning you first.

Colin

PHISHING = You receive a fake email purporting to come from your bank or Paypal, typically informing you that your account is about to be closed unless you click on a link and log in to confirm your details. The link actually sends you to a fake web site where they record your user ID and Password.