

Re: How do they blank out IP addresses etc?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2002-01/0612.html>

From: Gareth Jones (gareth@uberdog.net)

Date: 01/28/02

From: Gareth Jones <gareth@uberdog.net>

Date: Sun, 27 Jan 2002 23:57:41 GMT

John Perry <JohnPerry@redoak.co.ukNOSPAM> wrote:

>I received this HTML mail from a hotmail user but I've changed my email

>to zzzz and the originator to yyyy.

>

>How did he do this? No originating IP address and no audit trail at

>all. Any tips guys?

>

>MIME-Version: 1.0

>Content-Type: multipart/alternative;

> boundary="-----=_NextPart_003_01BOAKAT.8D5BF46A"

>Subject: =?windows-1252?Q?New msg ?=

>Date: Fri, 25 Jan 2002 11:13:00 PST

>From: yyyy@hotmail.com

>To: zzzz@hotmail.com

>X-Originating-IP: []

This is not the full header. Perhaps your email program doesn't display it all? The From: field is set by the sender – it is trivial to forge. You should have a series of from headers somewhere. Some of these might be faked, but at least one must be real...

Gareth

- **Next message:** [Darius Blaszyk: "Someone changed my dialup settings!!"](#)
- **Previous message:** [chris@nospam.com: "Re: How do they blank out IP addresses etc?"](#)
- **In reply to:** [John Perry: "How do they blank out IP addresses etc?"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)