The nasty people who flood our e-mail with unwanted advertising have been using increasingly
debceptive means to elude spam-filtering software, most of which runs on the same principle as
signature-based antivirus software or misuse-detection intrusion detection systems. The
defensive products rely on intelligence from the field to identify known patterns of subject lines
and content to screen spam from their users.

A simple technique that spammers have used recently is to find synonyms for the keywords that
are blocking their junk; thus they may use the chemical or generic name of various drugs instead
of the brand name. To avoid blockage of this message by readers’ antispam tools, I won’t give
specific examples here. The names are also spelled wrong in a wide range of ways – not by
mistake, one can be sure. Antispam products may have to extend their search strings to include
likely misspellings of key words.

Some spammers are shifting to almost exclusively HTML e-mail with embedded images that
represent their text. Thus instead of being able to scan for the keywords that characterize so
much of this repetitive garbage, the antispam tools are faced with bland HTML for a couple of
links and an unscannable bit-image that contains no machine-readable text.

Here, for example, is the source of an unwanted advertisement for a drug (by the way, you’d
surely have to be mad to trust a drug from an organization that sends spam):

```html
<html>
<body>
<center>
<!--yk4a733d3eykjav-->
<a href="http://www.ABCDE.com/host/default.asp?ID=omni">
<!--srYOQNvJ5H0n-->
<img src="http://FGHIJ.com/pics/gv1.gif" height="270" width="405">
</a>
</center>
</font>
</html>
```

Note that I took out the actual domain names in case your antispam filters have already included
them as forbidden strings.

The gif contains the actual advertisement – but how to read it? I think the only strategy that will
work for now is to have constantly expanding lists of the domains where the spam originates.

***
MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.