In the first four articles of this series, we have been looking at the problems raised by scumware—software that makes unauthorized changes to Web pages and other documents. In this, the last of the series, I will summarize measures for preventing and removing infestations of scumware.

First, you must decide if you approve of having advertisements and hyperlinks inserted into the views of Web pages that appear on your screen. If you do, there’s no problem and you can stop reading this column.

For those who don’t like the idea of extraneous links and ads, the most obvious measure for preventing infestation is not to install scumware at all. Unfortunately, this is not as easy as one would like. As we have seen in previous articles, scumware can infest other software and be installed with little or no notice to the user. Nonetheless, before installing freeware, shareware, or adware (products that offer services in return for sending the user targeted ads), everyone would do well to read about the product using an Internet search engine such as Google. Check the lists of known scumware at Scumware*Links <http://www.freegraphics.com/zz-scumware/> to see if the product you are thinking of installing is a known offender. Without gritting your teeth too hard, read the end-user license agreement (EULA). Look for language, no matter how convoluted or how tiny the point size, that indicates that the product is likely to add to or modify the appearance of Web pages you download. In addition, look for language that threatens to delete or inhibit any of your _other_ programs. As I was completing this article, Declan McCullagh’s admirable PoliTech list published a fascinating glimpse of the mindset of some adware makers. The RadLight adware product comes with a EULA that reads in part, “You are not allowed to use any third party program (e.g Ad-aware) to uninstall application bundled with RadLight. Such programs will be removed.” See http://www.politechbot.com/p-03439.html for details.

While you are installing _any_ software, from no matter what source, always keep your firewall active if at all possible. Be sure to configure your firewall to alert you to any attempt to contact an external address from inside your system; although such attempts may occasionally be necessary (e.g., for updates to critical components), in many cases they can be blocked safely. You can always study the issue more closely if necessary by examining the TCP address of the target and doing a reverse IP-block lookup to find out where the critter is trying to connect. Once you know the name of the registrant and the Domain Name System entry for the target, block the transmission without hesitation if you don’t know why a module on your system is trying to communicate with a site you know nothing about. You can always reverse your decision later if you determine that the connection is in your interest.

To identify undocumented or forgotten adware, spyware and scumware, several real-time scanners can spot trouble for you. For example, Lavasoft makes Ad-aware, a simple, free and
reliable product that scans your system for unwanted intruders and removes these programs from

* * *

technical bookstore or from Amazon <http://www.amazon.com/exec/obidos/ASIN/0471412589>

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 <mkabay@compuserve.com>. He invites inquiries about his information security and operations
management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information
technology, security and management.

Copyright © 2002 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.