Consequence-Avoidance Tools

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In my last column, I described the “privacy” software which I called “MyLittleSecret.” It includes stealth capabilities to conceal the presence and operation of the program from system administrators.

From my perspective in system management, MyLittleSecret is not so much “privacy protection” as “consequences avoidance.” It seems to me that this product is being praised by people who want to violate corporate appropriate-use policies. For good reason, network managers are concerned about the use of corporate resources for unauthorized Internet browsing: employees are being paid to get useful work done but are visiting sports sites, downloading pornography, and trading large volumes of music and video files. Wiping cache covers dirty tracks for people who are wasting time on unauthorized browsing, but it also eliminated cached copies of legitimate pages and symbols and can significantly slow down the next visit to a particular Web site.

The activities the stealth-mode software is covering are inherently risky. For example, in a bandwidth-bound organization, the extra load on Internet-connection bandwidth and even local area network bandwidth from unauthorized, heavy-duty browsing can slow response time for everyone on the network. Some of the materials being downloaded may make the employer liable for civil damages or criminal prosecution; trafficking in child pornography, for example, is illegal around the world. Even if these stealth products do wipe out traces of incriminating evidence, displaying objectionable material in the first place may itself contribute to what lawyers have called a “hostile work environment” and lead to lawsuits.

“Stealth mode” is designed to help the user avoid detection by duly constituted network authorities; the unexpected consequences are potentially serious. For example, from a support standpoint, if anything goes wrong with the stealth software, or if it interacts badly with other software, tech support may not identify the origin of the problem if the cause is hiding itself and users fail to mention its existence. If the corporate computer is passed on to another user without a thoroughgoing re-installation of the operating system, the stealth software may continue to load without any sign to the new user except for disappearance of cache and cookies – which may not be the desired condition. “Why do I keep having to write in my account information all the time??”

In the next column, I’ll finish off with a few suggestions on policy for coping with this nuisance.

* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see <http://www3.norwich.edu/msia> for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management 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 © 2005 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.