Digital Forensics (2)
by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

A journalist from South Africa recently wrote to me with a series of interesting questions about forensics and I had such fun answering that I got his permission to post his questions and my answers in a previous column and this one.

>Who’s doing the computer crimes?<

No one is very sure about that. There is no centralized reporting system where everyone is required to register attacks on their computers. All published research suffers from difficulties of ascertainment because of self-selection of those who respond to questions. In addition, we know from historical records that some crimes are not noticed until much later, if at all. Up until recent years, it has been a dogma in the information security field that most computer crimes (i.e., crimes against computers as targets and crimes using computers as tools) were perpetrated by employees authorized to use the systems they attacked or damaged. However, the enormous growth of the Internet has changed the views of some experts, myself included, so that we guess that we have probably crossed the boundary now and have more crimes committed by an outsiders than by insiders.

In general, motivations for computer crimes fall into three major categories:

* vandalism
* voyeurism
* greed.

What little research there is suggests that there is no one personality type or demographic absolutely tied to any of these categories. For example, vandals who launch denial of service attacks do include children with no ulterior motive, but they may also include adults attempting to extort money in a kind of modern protection racket. Similarly, there are teenagers who break into systems for fun; others are beginning to do so for-profit. Some people spreading lies on the Internet have done so simply out of free-floating ill will; however, quite a number have been involved in pump and dump schemes designed to drive the prices of selected stocks up or down so they could make illicit profits.

>How can ordinary users protect themselves from being used as stooges for online scams?<

Number one -- and I hope you will stress this -- don't give out confidential or private information to strangers. Don't give people who call you on the phone your bank information or your credit card numbers -- no matter how convincing they sound. Don't reveal passwords to anyone: no official will ever need to know your password -- they can get their work done in other ways or they can reset your password to a temporary value that will then force you to assign a new secret password that nobody else knows.

Second, install an effective antivirus program and configure it to update itself automatically every day.
Third, install a personal firewall on your computer; a simple but effective free firewall is available from ZoneLabs. When the firewall asks you if a program can access the Internet, answer no unless you know exactly which program it is and why it wants to reach outside your computer. Similarly, if the firewall asks you if someone can access your computer from the Internet answer no unless there is a very good reason for saying yes and you are absolutely sure you know what you are doing.

* * *

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 © 2004 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.