Frauds and Hoaxes: 4-1-9 Redux

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

This is the second of two short articles about hoaxsters abusing their victims’ good faith via e-mail. It ends with some suggestions on software installation policies.

* * *

I can’t tell if it’s just me, but the number of Nigerian 4-1-9 fraud letters I’m receiving has been growing to the point where I receive at least one pathetic letter per day telling me about how some creep in a developing country (Nigeria, Ghana, Mozambique, to name a few) has found or inherited a huge cache of illicit money skimmed off from the starving masses. In return for my revealing full details of my name, contact information and bank account details (yeah, right!), these self-avowed criminals will transfer amounts such as $50 million into my very own personal bank account and then move it out in a money-laundering scheme. I will supposedly benefit by keeping some large percentage (10%, 20%) of this stolen money. The scam is generally referred to as a 4-1-9 because of the applicable Nigerian laws governing fraud.

First off all, only an astonishing gullible person would give anyone, let alone a self-avowed embezzler_, details of their bank account. Second, only a larcenous twit would actually send anyone money for the fees and bribes demanded by the fraud artists – yet thousands of people have actually fallen for this scam, which has been around for over 20 years. A few American victims have spent up to tens of thousands of dollars on the illusory ill-gotten gains; a very few have traveled to Nigeria (in particular) and promptly been kidnapped and held for ransom. For more information about this nonsense, see the “419 Coalition Website” at <http://home.rica.net/alphae/419coal/> where you and your users can find a concise description of the fraud and an extensive list of links for further details. The FBI also has a number of informative pages on the scam; e.g., <http://www.fbi.gov/contact/fo/nyfo/fraudalert.htm#nigerian>.

* * *

A quick word about a KLEZ-related hoax that has been circulating lately: Some vile human being has written a convincing e-mail message that claims to have an anti-KLEZ program attached to it and appears to come from Kaspersky Labs, a well-known antivirus company. The subject line of the message is, “You're under a serious threat!” and the text reads, “Kaspersky Labs urging users to take the necessary measures to protect themselves against the mounting threat from the latest version of the Internet-worm Klez, most users lightly regarded the problem of securing their personal data, resulting in a global Internet virus epidemic. Over the past several days our technical support services have received over twelve thousand inquiries concerning Klez Internet worm infections.” As you can guess, the message is a lie; the attached file is actually a remote-access Trojan (RAT) called Smokedown. For full details see <http://www.kaspersky.com/news.html?tnews=20146&id=700915>. 
In general, it’s preferable to install software on your users’ computers using direct installation (physically at the system) if numbers allow this or using automated installation methods for computers with persistent intranet access. An alternative is to post digitally-signed executables on your intranet rather than using e-mail. If you do choose to send executables by e-mail, (1) send out a notice announcing that the software will be arriving; and (2) warn your users that you will _never_ distribute a copy of an executable by e-mail without a digital signature that can be verified.


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.