Reader Mark Heinrich, CISSP recently wrote, “Just after reading your column, I clicked to my next piece of email, a tacky bit of spam reminding to remit my outstanding (but unspecified) payment to the Nigerian National Bank by contacting someone at <e-mail address removed>. Is there someone I can forward this tripe to for investigation, prosecution, or perhaps a terrible accident in a dark alley? I remember long ago that the FBI had an e-address to forward things like this, but I do not know if that is still true. Do you have any suggestions for spam recipients?”

This simple question led me not only to review current resources for readers to use in informing your colleagues (and families and friends) about the notorious 4-1-9 advance-fee fraud, but also led to a brief demonstration of how to check for a possible phishing scam.

The reader is probably thinking of the Internet Fraud Complaint Center at <http://www1.ifccfbi.gov/index.asp>.

If you are looking for US law-enforcement agencies to contact, you can find an extensive table showing where to report which kind of Internet-related crime at <http://www.cybercrime.gov/reporting.htm>.

The National Consumers League <http://www.nclnet.org/> has created Fraud.org to help fight Internet and telemarketing fraud. They offer an Online Incident Report Form <http://68.166.162.20/repoform.htm> where victims can report online and telemarketing frauds.

Incidentally, you might be having the same reaction as I did to that funny looking URL with the IP address in it. My first reaction was to wonder if I was looking at a phishing scam, especially once I realized that all the other links on the page at <http://www.fraud.org/> use normal alphanumeric URLs. Could someone have hacked the legitimate Web page and linked to a bogus data collection site?

I looked up the <fraud.org> domain using the _whois_ service of InterNIC <http://www.internic.net/whois.html> and verified that it was indeed registered by the National Consumers League. Then I did a reverse IP lookup on <68.166.162.20> using SamSpade v1.4 (see <http://www.samspade.org/ssw/>) and found that the address resolved to a block owned by Covad Communications in San Jose, CA. I called the abuse line, where a very nice lady listened carefully to why I was asking for information about the IP address and confirmed that it is in fact owned by the National Consumers League. So I guess it’s not a phishing scam after all.

Anyway, how do I respond to fraudulent offers like the one my correspondent mentioned?

Well first, I subscribe to the Cloudmark Safetybar community <http://www.cloudmark.com/>
and so if a 4-1-9 advance-fee fraud or phishing message gets through their filters at all, I hit their “Block Fraud” button in my Outlook toolbar to simultaneously file the message in the spam folder and send notification to the central servers so that the new rubbish can be fingerprinted. The hash is then rapidly distributed to all of the million-plus subscribers (1.2 million as I write this).

Sometimes, if I have a moment, I sometimes forward particularly offensive fraud letters to <abuse@isp.dom> (where “isp” is the Internet service provider and “dom” is the domain for the return e-mail address used in the body of the fraudulent message) with a suggestion that they cancel that account to reduce the number of foolish victims. However, this technique doesn’t always work (sometimes the messages bounce) and in any case, I have to say that there are so many of these things that I rarely bother anymore.

* * *

For further reading

CIAC Hoaxbusters on 4-1-9
<http://hoaxbusters.ciac.org/HBScams.shtml#nigerian419>

United States Secret Service advisory about 4-1-9 scams
<http://www.secretservice.gov/alert419.shtml>

Urban Legends (snopes) on 4-1-9
<http://www.snopes.com/crime/fraud/nigeria.asp>

* * *

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.