April Fool’s Lessons

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

The day before April Fool’s Day (AFD) this year, one of my colleagues and I conspired to play a trick on our friend and colleague Dr Peter Stephenson, PhD, CISM, CISSP, FICAF, Associate Program Director of the MSIA program at Norwich University – and I have his kind permission to tell you about it.

Peter was in the process of updating curriculum materials for our seminars but had fallen behind schedule due to his enormous range of obligations (which include his being the CISO at Norwich). I had offered to help, but as usual, he said no, he’d deal with it. So I went ahead and spent 90 minutes on the Monday before AFD fixing the materials and checking all the links in the optional readings and bundled them up and sent them to our colleague along with a forged e-mail message (devoid of headers) dated AFD at 04:02 AM. She, in turn, was primed to send a reply to this fake e-mail early in the morning on AFD thanking him for the materials: “Thanks for your help with this project that just doesn’t want to go away. I know how much you have on your plate and I really appreciate that you took the time to do this. That you took additional time to check the optional readings is real dedication.”

It worked perfectly.

He was frantic: “Folks… I DID NOT SEND THIS… and I have not yet done it… we have a major problem here. It is on my plate for today and you likely would have gotten a message like this about the same time tomorrow morning but I repeat, I DID NOT SEND THIS MESSAGE. I need for you to capture the full headers on this (if you don’t know how, call me and I will talk you through it). This message either is spoofed or I have been working in my sleep!”

We called him up and expressed befuddled concern. “How could it be a spoof?” we asked earnestly. After all, it included valid curriculum materials. Was he sure he hadn’t just forgotten about sending the message? After toying with him for a few minutes, I said in a flash of apparent inspiration, “I know! It’s the GOOGLE e-mail option! You sent the e-mail back in time!” That tore it and we all had a good laugh.

For those who haven’t heard about it, GOOGLE had some hilarious spoofs on AFD, including “custom time” on its GMAIL site about a supposed new option that would not only allow backdating e-mail – it would actually allow sending it back in time!<<http://www.networkworld.com/news/2008/040108-google-april-fools.html>

Well, to end this cheerful little essay with at least something other than laughs, Peter and I did think up some meaningful lessons from the little prank.

First, the prank was possible only because Peter was not signing his e-mail messages with a digital signature. I use PGP to sign all my work-related messages and most of the rest of my e-mail (I avoid PGP signatures for stuff I send to naïve users who might be intimidated by the sig block)(one elderly correspondent asked me if “SHA-1” was Hebrew). So lesson number one is to
use digital signatures on your e-mail.

Second, we discovered during our conversation that Peter thought he _was_ signing his e-mail with PGP! Turned out upon examination that Outlook 2007 rejected the PGP add-in but he never noticed that his outbound mail was not in fact being signed. So lesson number two is to check that your security measures are actually working.

Lesson number three is that pranks are best when they’re friendly!

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2008 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.