LSI Journal

LSI's Experiences With E-Mail Scams

Editorial Comment by Warren Krug *(May-June, 2007)*

At its best the Internet is a wonderful tool that can provide users with all sorts of information and entertainment quickly and easily. At its worst it is a device that unscrupulous people are using more and more to literally rob innocent citizens of their hard-earned money.

We think this matter is important enough to share our own experiences with apparent attempts to steal our funds. Hopefully, our readers, if they aren't already well versed on Internet scams, will be better prepared if they too should face similar situations.

Offers of Big Donations

From time to time we have received offers of big donations from "wealthy" people "about to die" who are looking for a good Christian organization that could make good use of their inheritances.

Usually we have ignored these offers. Once though we decided to respond to an e-mail message from Saudi Arabia, thinking this might be an opportunity to preach a little Law and Gospel.

The e-mailer claimed to be dying of cancer, was a widow, had no heirs, and was a born-again Christian. Quoting a few Bible verses, the lady said she wanted to donate her sizable inheritance to LSI.

We responded with our sincere condolences, said we could send no money for taxes or lawyer fees, and gently reminded the woman that scams called for sincere repentance for which there is forgiveness.

Much to our surprise she replied. She indicated it would only be necessary to have one of our officers listed in her will so as to get the inheritance.

We briefly discussed this matter at a Board meeting, and some of the men smelled a trap though we couldn't put our finger on what it was.

We decided to inform her that we could only accept a direct donation in the form of a check or money order and could not allow any officer to be listed on any legal document.

We've never heard from her again. If any of our readers know what the trap could have been, please let us know.

Phishing

Recently we received an e-mail which looked to all the world like a legitimate message from our credit card company, the Bank of America.

The message asked us click on a link that looked like it would take us to the Bank of America Web site in order to update our credit card information. We would have to do this within 48 hours, or they would regard our account as fraudulent and close it.

Believing that a reputable credit card company would never be sending an e-mail of this type, we called Bank of America and were told it sounded to them like an example of phishing. This was verified after we sent the Bank of America a copy of the suspicious e-mail.

Phishing is an attempt to steal sensitive personal or financial information via e-mail.

Bank of America sent us the following clues that can help identify phishing:

--Does the e-mail ask you to go to a website to verify personal information?
--Does the message sound threatening? Ours did and most phishing e-mails do.
--Are there misspellings, bad grammar, or poor punctuation? Ours didn't have any of these errors.
--Are the links deceitful? By moving your cursor over the link you can tell. When we moved our cursor over the link that looked like a link to Bank of America, a completely different address showed up in the bar at the bottom of the screen.
--Is the e-mailer ignorant of your name? Our e-mail said only "Dear Customer."
--Is the sender's e-mail address suspicious?

Hopefully, this information will be prove helpful. *LSI*