

Easy marks

Why nonprofits are falling victim to a new fraud scheme

You probably already know that some scam artists “phish” or send e-mails, purporting to be from a legitimate charity, to individuals in order to gain donations or sensitive personal data such as credit card numbers. But you may not be aware of a relatively new phishing scam that’s putting nonprofits themselves at risk.

Be warned

In January 2008, the IRS issued warnings about e-mail scams targeting nonprofits. One bogus e-mail message purports to come from the IRS and claims that the recipient is eligible for a tax refund.

The messages are often customized to include paragraphs that refer to organizations that distribute funds to other organizations and appear to be signed by the director of the IRS’s Exempt Organizations division. The message contains a link where recipients are asked for sensitive information.

Another scam involves e-mails with attachments that the sender claims explain new tax laws. In reality, these attachments release malicious content such as viruses and spyware on the recipient’s computer.

The IRS has posted on its Web site (irs.gov) details regarding these and other schemes in which perpetrators have claimed to be from the IRS. The agency explains that it doesn’t reach out to taxpayers — to individuals or organizations — through e-mail. So be wary of any e-mail message that appears to be from the IRS and forward suspicious ones to phishing@irs.gov.

Don’t overlook your responsibility

In addition to taking defensive measures against e-mail scams, nonprofits also need to ensure their own e-mail communications are above suspicion. Your reputation as a legitimate nonprofit is on the line. To avoid looking like a phishing e-mail:

- Send e-mails only to those individuals who have opted in to your e-mail list,
- Include all contact information for your group in the message, including a phone number, mailing address and Web site address,
- Include a link to your written privacy policy, and
- Avoid sending attachments with e-mails.

Also take steps to minimize opportunities for scam artists to hijack your name and use it to solicit phony donations. In 2005, fraudsters set up a bogus United Way Web site that accepted donations, using the URL www.unitedways.com. They made the assumption (correct, in some cases) that people wouldn't notice the extra "s."

Consider registering common variations of your organization's name to make them unavailable to scam artists who want to capitalize on your public image. This might be overkill for small, local organizations, but worth the investment if your size, scope and public profile put you at risk.

Be safe, not sorry

Always think twice when asked to supply sensitive information, even if the request seems to come from a legitimate source. This can keep you out of the clutches of criminals intent on stealing your organization's assets and good name. Caution also puts you in a better position to reach out to your constituencies without setting off their alarm bells.