Prof Julie Tower-Pierce of Norwich University’s Justice Studies Department recently introduced me to a new word: “vishing.” According to Brian Bergstein of the Associated Press, “Internet con artists are turning to an old tool — the phone — to keep tricking Web users who have learned not to click on links in unsolicited e-mails.”

Vishing is a contraction of “voice phishing” and it asks victims to call a phone number where confidential information can be recorded for later abuse. According to Bergstein, some of the frauds involve a phone call to the victim with demands for confidential information such as credit-card security codes.

In my security courses, I teach students never to reveal confidential data to anyone who initiates a phone call. It’s one thing to volunteer to pay for something or to donate to a charity when you call an established, documented and credible phone number, but it’s too easy to fall prey to social engineering when you receive a call.

If you like a charity that is ostensibly calling you, ask them to send you documentation in the mail or go online yourself (look up the organization yourself rather than just copying down a Web address you are given over the phone). If you are unfamiliar with the organization, you can do a DNS lookup (I use the SamSpade utility for Windows but you can find many whois services using any search engine) and check the ownership of the site.

For more information on a purported charity, use the reports available from the Charity Reports of Give.org where you can obtain some sense of whether an organization is legitimate. Another good site is the Charity Navigator. I personally used these sites and others when I investigated a “charity” calling itself the American Veterans Coalition. You’ll be interested in the investigators’ findings: most or even all of the money collected is used for expenses — including salaries for the owners of the “non-profits.”

Be warned.

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information