The Norm Coleman Web Crash and Full Disclosure
Part 1: The Facts

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

How do we make ethical decisions? It is surely not by announcing preferences as if we were choosing a flavor of ice cream. There are guidelines we can follow in making ethical decisions, as Prof John Orlando, PhD described in an earlier series in this column in 2007 on social engineering in penetration testing.<http://www.networkworld.com/newsletters/sec/2007/1022sec2.html>

This column is the first of two articles written in close collaboration with MSIA student Becki True, CISSP examining the ethical questions raised by the actions taken by people who discovered a vulnerability on the Norm Coleman for Senate Website and made it public. Ms True and began with her initial essay and worked together in adapting and extending it for this series.

Before we go on any further, we want to make it clear that although we identify a specific blogger in these essays, our interest is not in character assassination; we are interested in using the incident as an opportunity for teaching.

* * *

In January 2009, there was a problem with the colemanforsenate.com Website. The site was unavailable and the Coleman people made a statement to the press stating that the site crashed due to “a flood of info-seeking disenfranchised voters.” <http://minnesotaindependent.com/24761/disenfranchised-voters-crash-colemans-site-unlikely-says-blogger> That statement led people to investigate and they found the site in a vulnerable state. Those who found the vulnerability publicized it on the Web using blogs, sent out messages via Twitter, and posted screenshots to Flicker. Ultimately, a donor database containing personally identifiable information (PII) such as names and associated credit-card numbers was downloaded and excerpts were posted on a Website.

This story is particularly interesting given the back-story. In the 2008 general election, Norm Coleman, a Republican, was the incumbent US Senator from Minnesota. The November 2008 election between him and his rival, Al Franken, the Democratic contender, was so close that it required a mandatory recount ultimately favoring Franken. Coleman disputed the election and took the fight to the courts but ultimately lost his appeal in the Minnesota Supreme court.<http://www.cnn.com/2009/POLITICS/06/30/franken.ruling/index.html>

Here is a timeline of events relating to the breach of the colemanforsenate.com Website.


2009-1-28: 4:55 PM: Twitter user @chuckmentary posts a Tweet commenting on the Coleman
article and includes a link to the news story. Information technology consultant Adria Richards, MCSA, MCDST, A+ (<http://adennetworks.com/about-your-consultant.html>) reads the Tweet and the article and decides to investigate. (<http://butyoureagirl.com/2009/01/28/did-norm-coleman-fake-his-own-Website-death/>)

2009-1-28: Sometime after 5 PM: Richards uses OpenDNS.com to find IP address of the colemanforsenate.com Website. OpenDNS returns 208.42.168.251. Richards enters IP address in her browser and begins her investigation. Instead of the expected content, Richards sees the directory listing of the file system. Richards knows something is wrong with the site.

At this point Richards had several choices. She could have:

- Attempted to find the site administrator using the DNS registrars (<http://www.betterwhois.com/>) and tried to contact the administrators
- Attempted to contact the Coleman office to notify them of the problem
- Attempted to contact the hosting company to have them take action

Instead Richards decided that this was what she called “breaking news” and she took a series of screenshots as she drilled down into the directory structure and uploaded the images to Flickr. (<http://butyoureagirl.com/2009/01/28/did-norm-coleman-fake-his-own-Website-death/>)

2009-1-28: 7:31 PM: Richards finds a compressed file named database.tar.gz and uploads screenshot to Flickr with the caption, “I wonder how much information is in this database at colemanforsenate.com?” (<http://www.flickr.com/photos/adriarichards/3234833407/>)

2009-1-28: 7:46 PM: Richard posts a comment on the Minnesota Independent news story that @chuckumentary included in his tweet. In her comment, Richards includes a link to the screenshots she posted on Flickr. (<http://minnesotaindependent.com/24761/disenfranchised-voters-crash-colemans-site-unlikely-says-blogger - comment-24110>)

2009-1-28: 10:40 PM: Someone calling themselves, “Epic” posts a comment to same news story that states, “Coleman just leaked his whole database” and includes a link to the database file. (<http://minnesotaindependent.com/24761/disenfranchised-voters-crash-colemans-site-unlikely-says-blogger - comment-24131>)

2009-3-10: Wikileaks.org received the database, which contained the unencrypted credit card numbers, names, addresses, e-mail addresses and phone numbers of donors. Wikileaks sent e-mail messages to donors alerting them of the breach and included enough information to establish their credibility. (<http://www.networkworld.com/news/2009/031209-former-senators-donor-database-exposed.html>)


In the second column in this pair, Becki True analyses the ethical reasoning that one could have followed in deciding what to do in this case and in similar cases.

* * *

Becki True, CISSP is a graduate student in the MSIA Program at Norwich University. She welcomes your comments. (<mailto:becki@beckitrue.com>)