Coleman's site wasn't 'hacked,' says IT pro who discovered donor breach

By **Paul Schmelzer**
Wednesday, March 11, 2009 at 12:59 pm

Former Sen. Norm Coleman Photo: WDCpix

Norm Coleman's campaign spokesman Cullen Sheehan suggested in an e-mail sent to supporters this morning that Wikileaks.org's publication of the campaign's donor database — including donors' credit card numbers and the three-digit security codes for those cards — is the work of politically motivated people who have "found a way to breach private and confidential information."

Sheehan hinted that the leak might be a work of political sabotage: "We don't know if last evening's e-mail is a political dirty trick or what the objective is of the person who sent the e-mail."

MinnPost's Joe Kimball echoed Sheehan's notion that the database was hacked, writing this morning that "some hackers (Web enthusiasts, [the Minnesota Independent] calls them), apparently discovered that list."

But the database was not revealed by hackers, according to IT professional Adria Richards, who was the first to share news of the unprotected file in late January.

"It's not hacking," she said. "I didn't use any hacking tools. A browser was my tool."

Richards said she discovered the database by entering colemanforsenate.com, into OpenDNS' cache-check tool, which gave her an IP address where the Web site lived.

Simply copying that address into a Firefox browser revealed the Web site directories for colemanforsenate.com.

Richards didn't download the database herself, but she posted a screen capture of what she'd found online after she made the discovery. An IT consultant for 10 years, she published her findings on her blog to educate others about the risks of improperly managed websites, she said.

"All you needed was a Web browser," she said. "It's like I walked over to Norm Coleman's house and saw his door was open, took a photo of the open door and posted it on the Internet."

Richards began her digging when sites like MNpublius and the Minnesota Independent started questioning a Coleman campaign assertion that its Web site crashed because of a traffic overload on a searchable database of voters "disenfranchised" in the U.S. Senate election that pitted Coleman, the Republican incumbent, against Democrat Al Franken.

The campaign's claims about the crash have been discredited, but Richards said she "noticed there was a bigger issue at hand than the site being down."

She said she's interested in Internet security, not in attacking Coleman, adding that she'd raise the same issues if anyone else, even a close friend, had the same type of Web security issues.

At least one local Web developer has downloaded the database from the Coleman site, which seems to contradict a Coleman campaign statement that no "unauthorized party" downloaded the database. That person won't speak on record for fear of prosecution by the Coleman campaign.

I clicked on the link to the database, which was provided by an anonymous commenter (not Richards) at MnIndy, but didn't proceed to download the contents.

What if I had? Would I be a hacker, to use Kimball's term?

"That's not hacking," Richards said. "If you can download Firefox from Firefox.com — if you download a picture from your grandma, you're downloading a file. Is that hacking? Five-year-olds can download files."

Further, she said she wonders why the Coleman campaign brought in federal authorities to see if there was a security breach, as Sheehan told supporters in this morning's e-mail.

"[Team Coleman's] traffic records should, could and would show if someone downloaded the file," she said. "You don't need the FBI to figure it out. Even Google Analytics show you what files people downloaded."

She's also skeptical about the campaign's comment about federal authorities checking the Coleman site's firewall. A firewall typically is used to grant or deny access to a server or network, not a database on a Web site.

The Coleman campaign has not yet responded to requests to clarify these issues.

Related:

Coleman donors express 'extreme anger,' fear, worry after breach

'Crashgate' reveals unprotected donor database on Coleman's site

Categories & Tags: Elections/Campaigns| Media| Politics| U.S. Senate| Add new tag | Adria Richards | Campaign Tech | Campaigns | Coleman breach | Joe Kimball | National/International | Norm Coleman | Wikileaks |

29 Comments

RSS feed for comments on this post.

Sorry, the comment form is closed at this time.