Browser tool Sell Hack gets C&D from LinkedIn

April 2 2014, by Nancy Owano

(Phys.org) —March did not exactly go out like a lamb for Sell Hack, which got a cease and desist letter from LinkedIn because the Sell Hack browser extension, once installed, could provide a pop-up button on LinkedIn profiles, where users could hope to get the account holder's email address, even if not connected. (SellHack is an extension compatible with Chrome, Firefox, and Safari browsers.) LinkedIn, said the BBC Tuesday, was advising users to uninstall it and request to Sell Hack to delete their information. The BBC reported that LinkedIn's legal team had delivered Sell Hack the cease-and-desist letter on Monday, March 31. SellHack responded Tuesday in a blog: "We have received a C&D letter from LinkedIn," the team said. "SellHack plugin no longer works on LinkedIn pages." The post also stated, "We are building a better product that does not conflict with LinkedIn's TOS." The team pointed out that "We only processed publicly visible data from LinkedIn based on your profile permissions… all of which has been deleted."

The Sell Hack posting also took the opportunity to note "We've been

described as sneaky, nefarious, no good, not 'legitimate' amongst other references by some. We're not. We're dads from the midwest [sic] who like to build web and mobile products that people use."

The Sell Hack blog motto read, "Save time and sell more! Uncover hidden email addresses and info using our browser extension's 'Hack IN' button on Social profiles." Their Twitter account refers to Sell Hack as a "Recruiters and Biz Dev productivity tool."

Sell Hack is a browser extension using JavaScript that seeks to garner email addresses associated with social media profiles from the web.

According to the site explanation of how it works: "Once you install the browser extension, any time you go to a Social profile page, you see a 'Hack In' button. If you click the button, we'll start to run the profile against our data sources. Often, we can return a validated email for you. If we don't receive a validation response, we'll present a 'copy all' button to copy & paste the list for your own uses."

Back in February, the Sell Hack team had used their blog to elaborate on what they were doing and who they were trying to reach, in a posting, "Why We Built SellHack."

"As a sales professional, I know the value of a warm intro and the opportunity cost of a non-connect." With the Sell Hack extension, they said, "The magic happens when you click the 'HackIn' button. You'll notice the page slides down and our system starts checking publicly available data sources to return a confirmation of the person's email address or our best guesses."

The blog said, "SellHack still saves me a ton of time. I don't have to manually create the different permutations of what the person's email address could be (ryan@, ryano@, rodonnell@ etc)."

Sell Hack also carried in its FAQ portion the question, "How is this legal?" The team's answer is that "The data we process is all publicly available. We just do the heavy lifting and complicated computing to save you time. We aren't doing anything malicious to a Social website. We think browser extensions are the best way to personalize an individuals [sic] web experience."

According to a LinkedIn spokesperson, said security analyst Graham Cluley,"no LinkedIn data has been compromised and Sell Hack is not the result of a security breach, bug or vulnerability."

© 2014 Phys.org