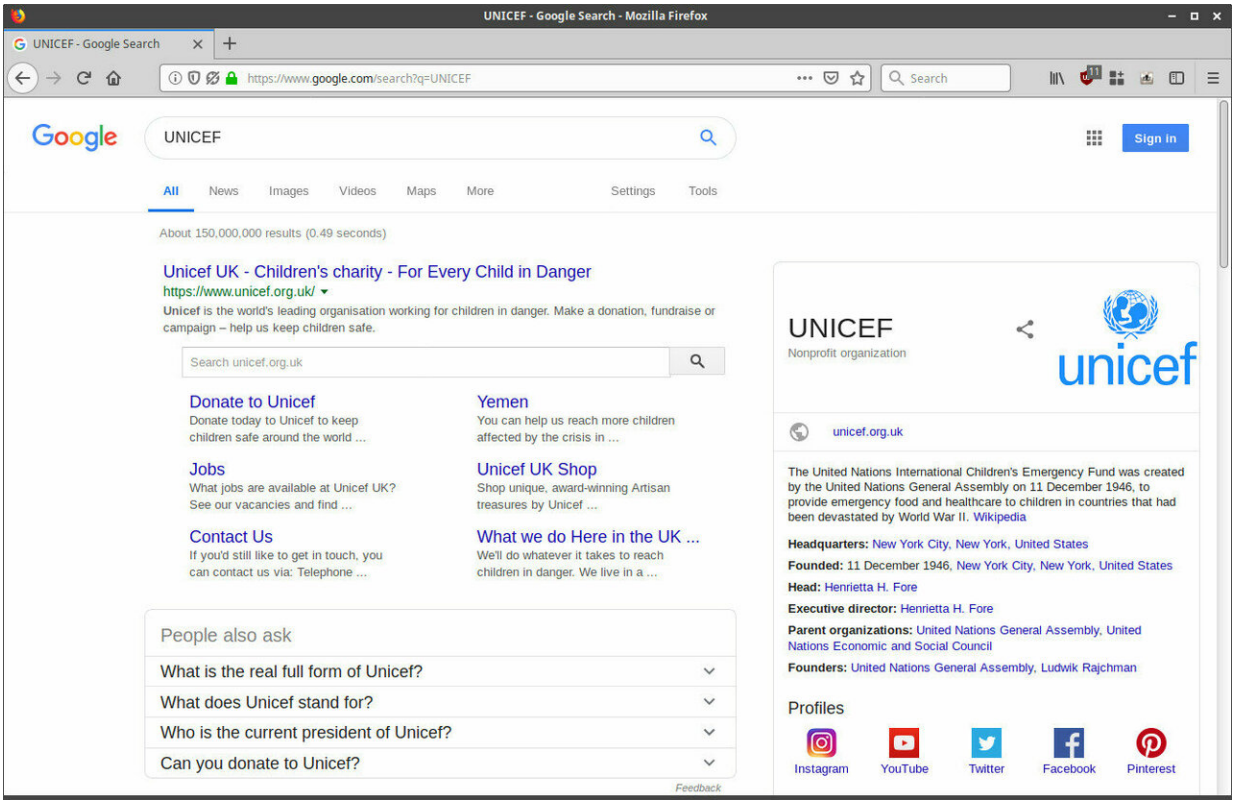
Fun tricks possible with Google knowledge boxes no laughing matter for some

January 11 2019, by Nancy Cohen



Example of a Google Search with a Knowledge Graph card on the right. Credit: wietzebeukema.nl

Google-watching hounds were understandably happy if not relieved to report that Google appeared to be responding to findings that a search engine bug was leaving the door open to spoofing, as pinpointed by

Wietze Beukema last year.

"Glaring 2017 Google Search Spoofing Bug Finally Getting Fixed" was the news from *Android Headlines*; *Search Engine Land* also reported that Google was working on it. So what was the fuss all about?

Google graph card search results could be spoofed to create fake news, said a number of sites including *Threatpost* on Thursday. How can a technique get away with a spoofing attempt? Tara Seals in *Threatpost* said it was "by simply adding two parameters to any Google Search URL."

Beukema blogged, "By adding two parameters to any Google Search URL, you can replace search results with a Knowledge Graph card of your choice."

For mischief makers hoping to inject the dis- as in disinformation, it appeared that a prize toy for their benefit could be in the Knowledge Graph, vulnerable to spoofs.

Ilonut Ilascu, *BleepingComputer*: "Knowledge Graphs come with a share button you can use to create a shortened link for easy distribution of the search query. The full URL includes a parameter ('kgmid') with an identification code for the Knowledge Graph card displayed with the Google results. 'As it turns out, you can add this parameter to any valid Google Search URL, and it will show you the Knowledge Graph card next to the search results of the search query,' says Wietze Beukema."

Researcher Wietze Beukema had brought up the topic of Knowledge Cards, which are boxes on the right-hand side of the search screen that contain relevant information to whatever search query a user types into Google Search. A search for a topic presents the regular search results but also with a Knowledge Card with key facts about the topic.

Also, said *Threatpost*, it is possible to create a URL that only shows the Knowledge Graph card and omits any search results, by adding the &kponly parameter to the URL results for any given query.

In the bigger picture, this is about Google not just something called a knowledge graph. Computer users rely on their Google Search to give them real, not deliberately spoofed, information. So, people were asking, what, could this be true, a spoofing technique that creates fake results? Some observers suggested this was apart from the usual headaches about falling victim to fake news; this was more difficult to figure out as the occurrence would involve not a person but a system that users trust.

If our media-imbibing brain were a weather report, it might possibly be in a permanent state of cloudy with a chance of being rendered clueless. As Daniel Golightly commented, "the company has largely built its reputation on the trustworthy nature of its searches."

Don't invite Beukema to any Salute to Knowledge Cards 2019. Beukema blogged: "Whilst the information often comes straight from Wikipedia, this is not always the case—unfortunately Knowledge Graph doesn't tell you where it got the information from."

However, it is easily presented as a boxed informaton and is rather effortless to view. In fact, he confessed, "I have caught myself relying on the information presented by Google rather than studying the search results, and I'm sure you have too."

"After all," he added, " it is a legitimate Google Search link and since we have been trained to trust the answers provided by Google, there must be some truth in it, right?" Wrong. And Beukema wanted to let Google know what was possible. Last year, he filed a bug report, said *Threatpost*. Seals said he advocated disabling "&kponly parameter in particular." As he wrote in his blog, "The bug report I filed about a year ago was closed

as it wasn't considered a severe enough vulnerability."

Daniel Golightly in *Android Headlines*, though, described a later turn of events, where "Google will finally be working to fix a bug in its search engine that allowed results to be spoofed and was first reported by Wietze Beukema in 2017." There is only one slight wrinkle to this happy ending. He did not know when. "But the search giant has not offered any kind of timeline for when the fix might be implementing," Golightly said.

Barry Schwartz is *Search Engine Land*'s News Editor and his January 9 post said, "A knowledge panel manipulation technique is finally getting the search giant's serious attention." He reported that a Google spokesperson told *Search Engine Land*, "We share the concern about the potential for bad actors to create misleading distortions of our search results pages, and are working to fix this issue."

Schwartz added that "We believe Google is now working on preventing this sort of manipulation in the search results. But we do not know how long it will take to resolve."

Meanwhile, it would be fair to point out that Roger Montti, SEO consultant, appeared to have another perspective on this. Montti pointed out in *Search Engine Journal* that one cannot really consider this ia hijack of Google's search results—not really. Why is it not a manipulation of search results?

The so-called exploit does not alter Google's search results at Google or for anyone other than the person looking at a specific URL.

"What this so-called hijack does is allow someone to play around with the URL parameters in order to generate a modified version of Google's search results," said Montti.

So, what is the relationship of the panel exploit to search results? "Modifying the URL parameters does not alter the search results at Google itself or for everyone. It only alters the search results for the person who is altering it themself or for a person who clicks through a link to that altered search result."

Verdict? "At best this is an amusing trick," Montti wrote. "It's yet to be seen if someone with malicious intentions could use it for negative ends."

More information: wietzebeukema.nl/blog/spoofing … oogle-search-results