Hijacked Google My Business listings appear to be a growing problem

The problem of hijacked Google My Business listings (GMB) – where someone other than the business gains control of the local profile – appears to be growing. SterlingSky's Joy Hawkins has reported on the trend and some of the methods used by spammers and scammers.

GMB phishing. Unethical local marketers are effectively phishing, using the "claim this business" link in the local Knowledge Panel/Profile. That generates an email request for control over the listing, which is sent to the registered owner of the profile. There are many examples and complaints on the GMB forum.

The frequency of this tactic appears to be increasing. In one of the examples cited by Hawkins, a hijacked listing for a law firm was used to sell leads to other personal injury lawyers.

Asked about this phenomenon, a Google spokesperson told Search Engine Land, "We're aware of this incident and are monitoring it closely and are continually working to keep the information on Maps safe and accurate. If a merchant ever receives a request to manage or to transfer ownership from an unknown person, they should decline the request. The rights to own or manage a Business Profile can only be granted if the verified merchant accepts the request or the requester proves their affiliation with the business."

Listings merger leads to unwitting "hijack"

Merger of ‘duplicates’ leads to unintended hijack. In another more obscure hijacking example, Rasmus Himmelstrup of Resolution Media in Denmark (Omnicom Media Group) told me he was able to take control of a listing from a large Danish supermarket chain, Bilka. This was not by design.

Himmelstrup’s client is a European optometry chain called Specsavers, which in Demark is known as Louis Nielsen. The grocery store, Bilka, and optical store were flagged as duplicates (by Google or a third party) and merged. The merged listing shows a mix of information for both locations: photos from both businesses, booking link for the optometrist, store hours for the supermarket and so on.

Himmelstrup said he reported the problem to GMB support and

was told to verify that the Specsavers location actually existed. He remarked to me that this response is “a good example of how inadequate the first line of GMB support is.”

Google reportedly told Himmelstrup to delete the duplicate and re-verify the Specsavers location, which he did. He added, “Upon verification I was granted access to the grocery store GMB listing instead, containing Specsavers info as well.”

Himmelstrup doesn’t want control over Bilka’s listing. Ironically, Resolution Media represents Bilka’s major competitor in Denmark and so if he wanted to, Himmelstrup could engage in all sorts of mischief. He wouldn’t of course, but, to date, he’s been unable to get Google support to fully understand the problem.

Why we care. Obviously, listings fraud, fake reviews and any other bogus local information in Google Maps and Search is bad for consumers. But it’s especially bad for the mostly small business (SMB) victims. Inaccurate online information can have a material impact on their sales, especially during COVID. For the many SMBs that are suffering ranking in local search results is a matter of survival.

It seems clear from looking at the GMB forum that business owners haven’t been sufficiently educated about the risks of hijacking and that Google needs to implement more SMB safeguards – and perhaps better training for its support people.

Related: How to optimize your Google local Knowledge Panel

About The Author

Greg Sterling is a Contributing Editor to Search Engine Land, a member of the programming team for SMX events and the VP, Market Insights at Uberall.

http://feeds.searchengineland.com/~r/searchengineland/~3/GRwljWNMJKI/hijacked-google-my-business-listings-appear-to-be-a-growing-problem-343737