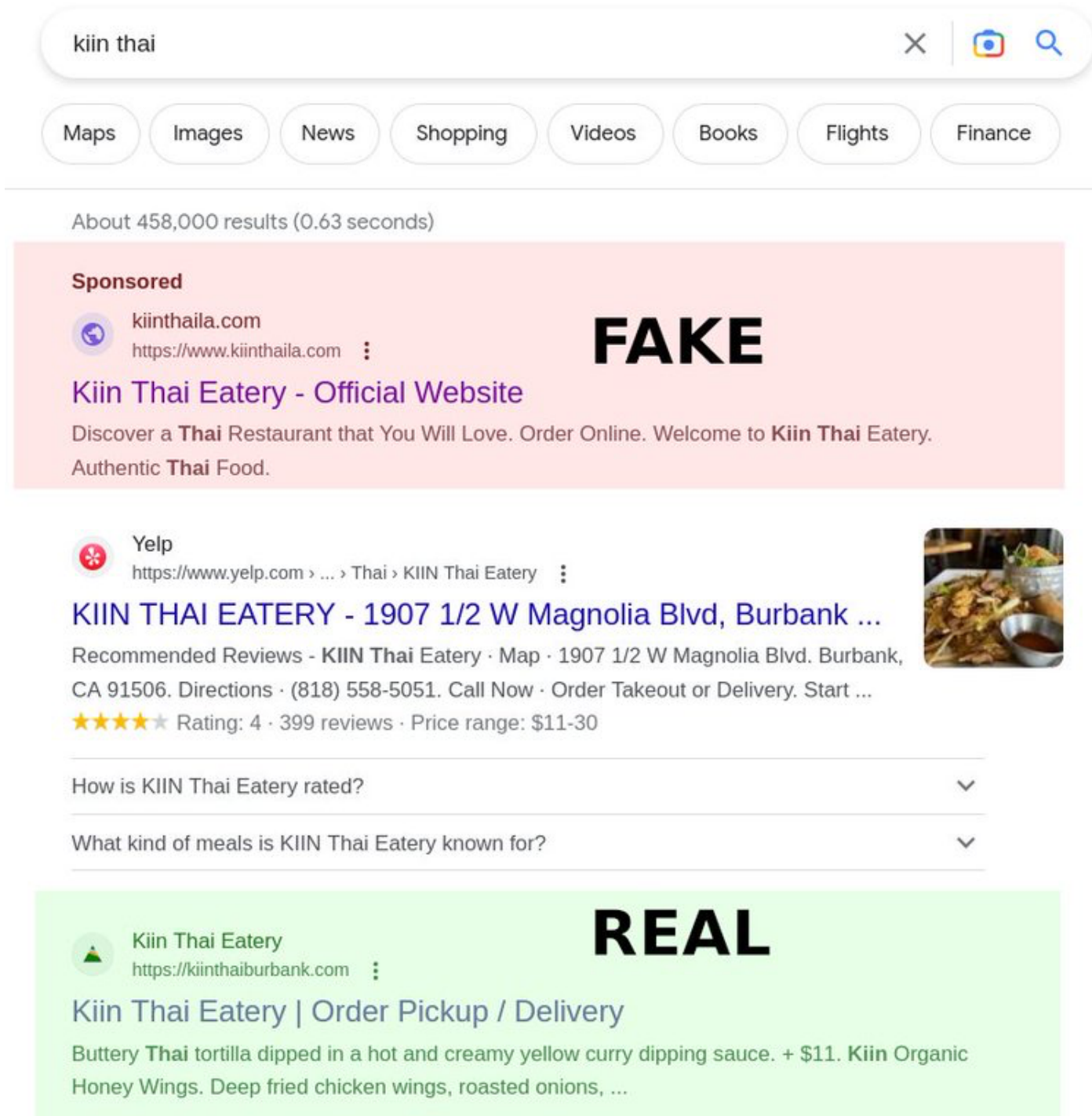


<https://twitter.com/doctorow/status/1628948906657878016>

Cory Doctorow @doctorow
Feb 23, 2023

So there's a great Thai restaurant in my neighborhood called Kiin. Yesterday, I searched for their website to order some takeout. Here's the Google result.



[Image Description: Screenshot of the results of a Google search showing a Sponsored Ad for a business called Kiin Thai Eatery above a regular Google entry for a different business also called Kiin Thai Eatery.]

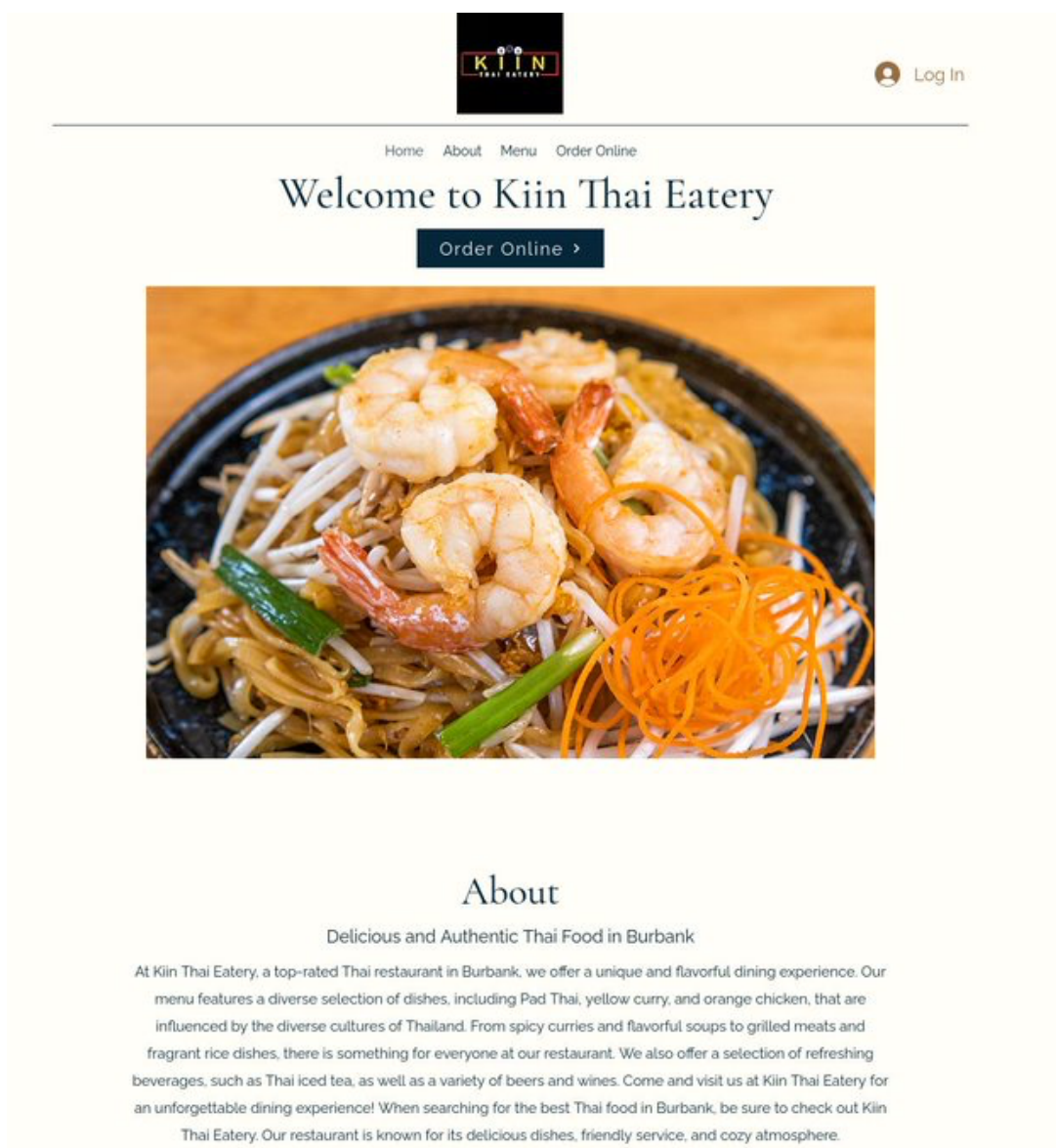
That top result (an ad)? It's fake. It goes to <https://kiinthaila.com>, which is NOT the website for Kiin.

The *third* result is real: <https://kiinthaiburbank.com>

Fake site:

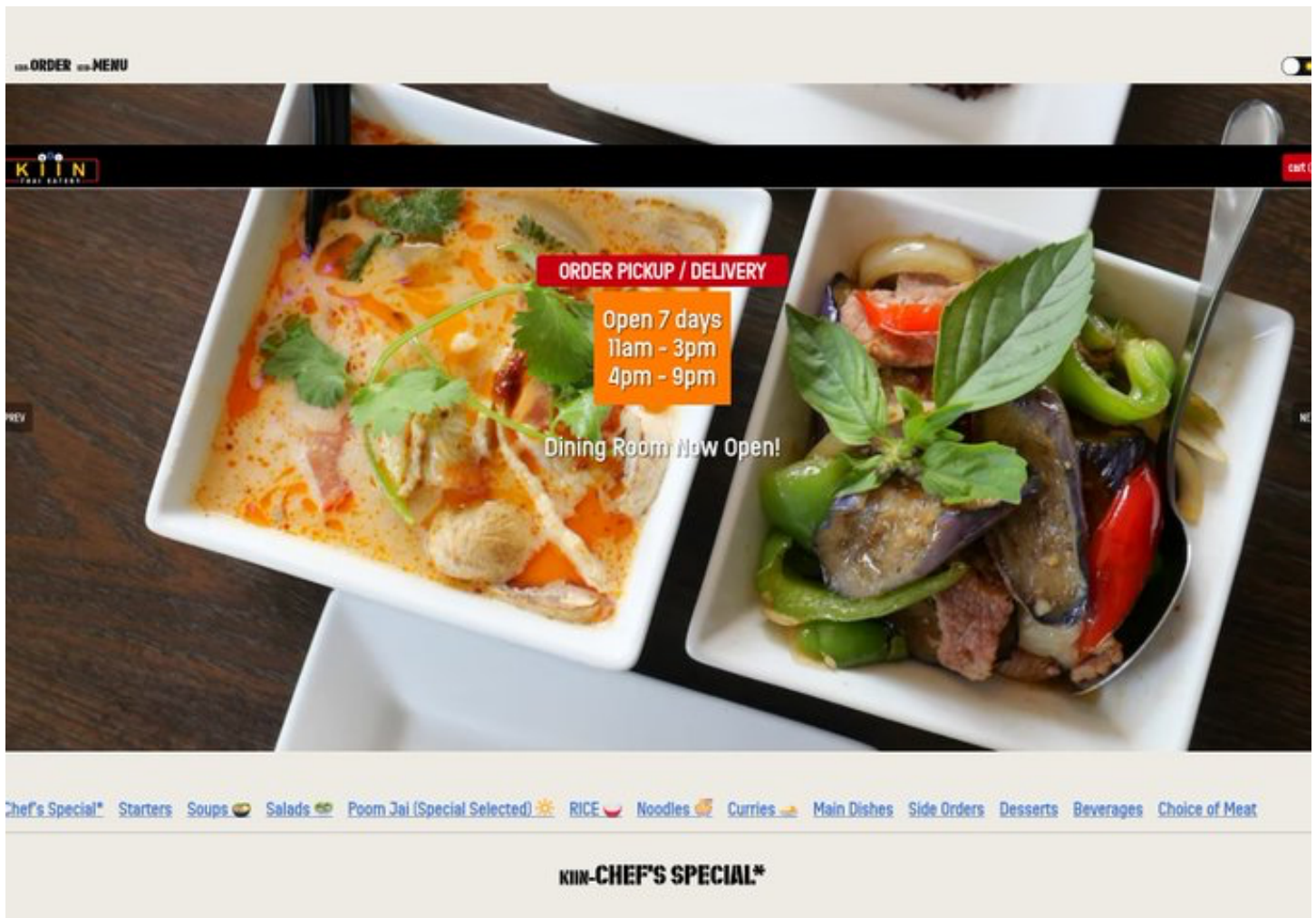


[Image Description: Screenshot of a logo for the “fake” business Kiin Thai Eatery.]



[Image Description: Screenshot of a webpage of the “fake” business Kiin Thai Eatery. Webpage says “Welcome to Kiin Thai Eatery” and has a picture of a noodle dish about an “About” paragraph.]

Real site:



[Image Description: Screenshot of a webpage of the “real” business Kiin Thai Eatery. Webpage says “Order Pickup / Delivery” and has a picture of two prepared dishes.]

I got duped. I placed an order with the fake site. The fake site then placed the order - in my name! - with the real site, having marked up the prices by 15%.

Kiin clearly knows they're doing this (presumably by the billing data on the credit card the fakesters use to place the order). They called me within minutes to tell me they'd cancelled the fakesters' order.

I could still come pick it up, but I'd have to pay them, and cancel the payment to the fakesters with @AskAmex [American Express Credit Card company].

Actually, as it turns out, I have to cancel TWO payments, because the fakesters DOUBLE-charged me.

Here's what that charge looks like on my Amex [American Express Credit Card] bill.

See that phone number? (415) 639-9034 is the number for @Wix [a website company], who provides the scammers' website [implying that the “fake” restaurant doesn't even have a physical location, just a website].

Pending

 Print

KIINTHAILA.COM

(415) 639-9034

[Visit Business](#)



Method:
Card used online

Rewards

You'll be able to see Rewards Information for an eligible charge within 5 days of the charge posting to your account. Please check back later.

Don't recognize this charge?

We can alert you by email once this pending charge posts to your account, usually within 72 hours of when it appeared.

[Alert me when posted](#)

Use Points for Charges

[Image Description: Screenshot of a credit card statement showing a charge from the "fake" restaurant and a contact phone number for the "fake" restaurant.]

How the actual [expletive] did these obvious scammers get an Amex merchant account in the name of "KIINTHAILA" by supplying the phone number for a website hosting company?

What is Amex's #KYC procedure? [KYC means "Know Your Customer" and it is, for many credit cards, a "mandatory process of identifying and verifying the store's identity."] Do they even call the phone number?

And why the actual [expletive] is @GoogleAds accepting these scam artists' ads for a business that they already have a knowledge box for?!

Google KNOWS what the real KIIN restaurant is, and yet they are accepting payment to put a fake KIIN listing two slots ABOVE the real one.

To be fair to these scammer [expletive] ripoff creeps who are trying to steal from my local mom-and-pop, single location Thai eatery, they're just following in the shoes of Doordash and Uber Eats, who did the same thing to hundreds (thousands?) of restaurants during [the pandemic] lockdown.

Doug @Rushkoff says that the ethic of today's "entrepreneur" is to #GoMeta - don't provide a product or a service, simply find a way to be a predatory squatter on a chokepoint between people who do useful things and people who use those things.

These parasites have turned themselves into landlords of someone else's home, collecting rent on a property they don't own and have no connection to.

There's NEVER just one ant. I guaran-[expletive]-tee you that these same creeps have 1,000 other fake Wix websites with 1,000 fake Amex merchant accounts for 1,000 REAL businesses, and that Google has sold them ads for every one of them.

Amex [American Express Credit Card company] and Google and Wix [website hosting company] should be able to spot these creeps FROM ORBIT. Holy [expletive] do we live in the worst of all possible timelines. We have these monopolist megacorps that spy on and control everything we do, wielding the most arbitrary and high-handed authority.

And yet they do NOT ONE [expletive] THING to prevent these petty scammers from using their infra as force-multipliers to let them steal from every hungry person patronizing every local restaurant.

I mean, what's the point of letting these robber-barons run the entire show if they're not even COMPETENT?

ETA [Edited To Add]: Dinner was delicious.