**CASE STUDIES – EQUIFAX**



In the aftermath of eruptive news that Equifax seemingly [had exposed](http://www.forbes.com/sites/janetwburns/2017/09/15/chatbot-helps-users-fight-parking-tickets-sue-equifax-for-up-to-25k/" \t "_self) the intimate data of 143 million Americans, it seems the credit-monitoring firm has also been lax on how it links customers with support.

Earlier this month, Equifax discovered that hackers had gained access to its info on more than 40% of Americans over the summer, so they set up a website where potential victims could check to see if they had been affected: [www.equifaxsecurity2017.com](http://www.equifaxsecurity2017.com/" \t "_blank). As [The Verge](https://www.theverge.com/2017/9/20/16339612/equifax-tweet-wrong-website-phishing-identity-monitoring" \t "_blank) pointed out, the page was not part of the greater equifax.com, and therefore posed a risk for users by requiring this voyage out to an external site.

In response, programmer [Nick Sweeting](https://sweeting.me/" \t "_blank) decided to highlight the vulnerabilities of the company's new site by exploiting the very same in a seemingly benign if striking way. He set up shop on  [securityequifax2017.com](http://securityequifax2017.com/" \t "_blank), a typo on the original site that consumers could easily reach by mistake, and created a faux version of Equifax's site for potential breach victims (but which didn't save any private info they might have entered). A headline on the site also read, “Cybersecurity Incident & Important Consumer Information Which is Totally Fake, Why Did Equifax Use A Domain That’s So Easily Impersonated By Phishing Sites?”

Sweeting explained in an email to the *[New York Times](https://www.nytimes.com/2017/09/20/business/equifax-fake-website.html" \t "_blank)* that using the Linux command "wget" makes it simple for anyone to download the contents of an entire website, “including all images, HTML, CSS, etc,” and impersonate that site.

“It was super easy to just suck their whole site down with wget and throw it on a $5 server,” Sweeting wrote. “It currently has the same type of SSL certificate as the real version, so from a trust perspective, there’s no way for users to authenticate the real one vs. my server.”

And in the past few weeks, Equifax itself was apparently taken in by the simulated website, or at least its typo URL. As the Verge reported, Equifax tweeted the link for Sweeting's [securityequifax2017.com](http://securityequifax2017.com/" \t "_blank) four times to potential breach victims who asked the company for assistance on Twitter, reaching as far back at September 9.

According to the Verge, Equifax deleted the tweets shortly after the website published its article about the mix-up yesterday.

By Wednesday evening, the fake Equifax site had been blacklisted by Firefox, Safari, and Chrome browsers, and Sweeting had taken it down. According to the *Times*, it had already received close to 200,000 hits.

Not only did they tweet the wrong link, they tweeted it 3 times. [#Equihax](https://twitter.com/hashtag/Equihax?src=hash" \t "_blank) [pic.twitter.com/T8jrhSfhqw](https://t.co/T8jrhSfhqw" \t "_blank)

— Nick Sweeting

CYBER SECURITY RISK MANAGEMENT - WORKSHOP











