Issued 9/21/17

For Weeks, Equifax Customer Service has been Directing Victims to a Fake Phishing Site

Earlier this month, hackers broke into Equifax's servers and stole 143 million people's personal information, including their Social Security numbers. In response to the attack, Equifax set up a website — www.equifaxsecurity2017.com — for possible victims to verify whether they're affected. Because the process involves sharing sensitive information, consumers have to trust they're entering their data in the right place, which can be tricky because the breach-recovery site itself isn't part of equifax.com. If users end up on the wrong site, they could end up leaking the data they're already concerned was stolen. Today, Equifax ended up creating that exact situation on Twitter. In a tweet to a potential victim, the credit bureau linked to securityequifax2017.com, instead of equifaxsecurity2017.com. It was an easy mistake to make, but the result sent the user to a site with no connection to Equifax itself. Equifax deleted the tweet shortly after this article was published, but it remained live for nearly 24 hours. Further research revealed three more tweets that had sent potential victims to the same false address, dating back as far as September 9th. These tweets have also since been deleted. Luckily, the alternate URL Equifax sent the victim to isn't malicious. Full-stack developer Nick Sweeting set up the misspelled phishing site in order to expose vulnerabilities that existed in Equifax's response page. "I made the site because Equifax made a huge mistake by using a domain that doesn't have any trust attached to it [as opposed to hosting it on equifax.com]," Sweeting tells The Verge. "It makes it ridiculously

easy for scammers to come in and build clones — they can buy up dozens of domains, and typo- squat to get people to type in their info." Sweeting says no data will leave his page and that he "removed any risk of leaking data via network requests by redirecting them back to the user's own computer," so hopefully data entered on his site is relatively safe. Still, Equifax's team linked out to his page. That isn't reassuring. Although the misspelled link likely wasn't intentional on Equifax's part, it demonstrates just how easy it is for attackers to trick consumers — even the company's own support team was fooled. It also shows a lack of a consistent response strategy. I don't necessarily blame the support team, as they're likely freelancers hired for this breach, but Equifax needs to get its response strategy together. An Equifax spokesperson says all tweets sent from their account with the wrong URL have been deleted. "All posts using the wrong link have been taken down. To confirm, the correct website is [https://www.equifaxsecurity2017.com]. We apologize for the confusion." If you're signing up for Equifax's identity monitoring, requesting a credit freeze, or inputting your personal information anywhere online, double check that you've navigated to the right webpage.