

Equifax Phishing Attacks

You already know that a whopping 143 million Equifax records were compromised. The difference with this one is that a big-three credit bureau like Equifax tracks so much personal and sometimes confidential information like social security numbers, full names, addresses, birth dates, and even drivers licenses and credit card numbers for some.

It can be the difference between being able to buy a house or sometimes even get a job or not. This breach and the way they handled it, including the announcement, was what Brian Krebs rightfully called a dumpster fire.

The problem is that with this much personal information in the hands of the bad guys, highly targeted spear phishing attacks can be expected, and a variety of other related crime like full-on identity theft on a much larger scale.

These records are first going to be sold on the dark web to organized crime for premium prices, for immediate exploitation, sometimes by local gangs on the street. Shame on Equifax for this epic fail. They will be sued for billions of dollars for this web-app vulnerability.

It is inevitable in the near future that we will see Equifax phishing attacks. The bad guys are going to take their most efficient way to leverage this data... email.

Cyber criminals have stolen 143 million credit records in the recent hacking scandal at big-three credit bureau Equifax. At this point you have to assume that the bad guys have highly personal information that they can use to trick you. You need to watch out for the following things:

- * Phishing emails that claim to be from Equifax where you can check if your data was compromised
- * Phishing emails that claim there is a problem with a credit card, your credit record, or other personal financial information
- * Calls from scammers that claim they are from your bank or credit union
- * Fraudulent charges on any credit card because your identity was stolen
- How to prevent identity theft:
 - * Sign up for credit monitoring (there are many companies providing that service including Equifax but we cannot recommend that)

* Next freeze your credit files at the three major credit bureaus Equifax, Experian and TransUnion. Remember it is not possible to sign up for credit monitoring services after a freeze is in place. Advice for how to file a freeze is available on a state-by-state basis: <http://consumersunion.org/research/security-freeze/>

* Check your credit reports via the free annualcreditreport.com

* Check your bank and credit card statements for any unauthorized activity

* If you believe you may have been the victim of identity theft, here is a site where you can learn more about how to protect yourself: www.idtheftcenter.org. You can also call the center's toll-free number (888-400-5530) for advice on how to resolve identify-theft issues. All of the center's services are free.