Protect Yourself from the Anthem Data Hack

Find me on:

Feb 26, 2015

IDENTITY

This article isn't for everyone - only eighty million of you (or78.8 million to be more precise). That's the whoppingly huge number of Anthem Health Insurance customers whose personally identifiable information (PII) is now in the hands of internet thieves. If you're a current or former Anthem subscriber (or a Blue Cross Blue Shield subscriber who received services from Anthem), crooks probably have your full name, birth date, member ID data, street address, phone number, email address, and employment information.

Armed with your PII, these criminals (or the people who buy your PII on the black market) are cooking up ways to steal from you. Here's a partial list of what they might be considering:

- Registering for credit cards under your name and going on shopping sprees.
- Foisting their income taxes on you. If a fraudster gives their employer your social security number, you're on the hook to the IRS for the crook's earned income.
- Obtaining government documents like drivers licenses.
- Stealing from your bank accounts. Once they can obtain a driver's license with your name and *their* photo, criminals can access your accounts.
- Using your credit to buy cell phones, cars, and apartment leases.
- Billing their medical claims under your name and account. You could be charged for someone else's gastric bypass or medical prescription.

To pull off these crimes, data crooks often need a little extra help and information from you. Be on the lookout for their most popular schemes.

Spearphishing -- This Time, It's Personal

In a typical phishing scam, a criminal will send you an impersonal email asking for your personal information.*Spear*-phishing is the same, except the email you get from the criminal appears to be from a legitimate company and has your name and other personal information in it. This personal touch makes it seem legit. You might trash an urgent email addressed to "Dear Sir," but one with your name and address in it might seem like something you should take care of right away.

Your (Fake) Bill Is Past Due

Since all of your recently stolen data is linked to Anthem, you might receive phishing or spearphishing emails with fraudulent health insurance bills. These messages will provide links for you to make these payments. However, the links won't take you to the Anthem site or the website of one of their approved vendors. They will go to sites that *look* like Anthem but are run by criminals.

Also, you may get emails, seemingly from Anthem, asking you to register for free credit monitoring protection. In fact, the links in these messages will try to trick you into providing your private login information or deploy malicious software on to your computer.

Spam with Drive-Bys

Equipped with Anthem subscriber email addresses, thieves can blast an "important message" with a nefarious link. If you click

on the link, you could unintentionally download malware that can spy on your keystrokes (a way to learn your passwords), steal stored credit card numbers, or even lock your computer and hold it for ransom.

Stay Safe. Use Restraint.

To avoid getting ripped off, there are some things you should **NOT** do. First, **DO NOT** click on any links in emails from companies. Second, if you do realize you've clicked on a link, **DO NOT** provide any information to the site where you land. Instead, open a new tab or window to access Anthem's site (or any other company's site, for that matter). Third, **DO NOT** reply to the email or offer the sender any information - this will only validate your address and encourage the criminals to target you more aggressively. Fourth, **DO NOT** open any attachments in an email from Anthem or from any suspicious senders. Legitimate emails will almost never include an attachment.

Also, be suspicious of phone calls telling you that you're a victim. Anthem has said it will contact all potential victims by mail. However, some people have reported getting calls from the insurer to discuss the data theft or overdue balances. These calls are almost certainly a scam.

If you get a call from Anthem or any other "company" asking for your personal information or your insurance details, ask for an 800 number to call them back. Next, run a quick Google search on the phone number to make sure it's legit. If you're satisfied with the results, return the call.

Always Protect Your Internet Connection

The best way to stay safe whenever you go online is to upgrade to a secure, cloud-based web browser. With this type of browser, a thief's clever phishing and malware attacks simply fall flat. A cloud browser prevents you from accidentally downloading nefarious software. Plus, you never have to type your passwords because your browser encrypts and auto-fills them through two-step verification and secure shortcuts.

If You're A Victim, Take Action

Restoring your life and finances after an identity theft is often a time-consuming nightmare. If you think you are the victim of identity theft, there are some things you should do.

For people affected by the data breach, Anthem has prepared an official website for information at**www.AnthemFacts.com**. It's also offering 24 months of identity theft monitoring and credit repair services through AllClear ID. Enrollment is available online, through a link from the AnthemFacts.com website.

In addition, the US Federal Trade Commission (FTC) has a site with helpful links and action steps. The FTC even has information specific to the challenges of medical information theft, which costs victims an average of $13,450.

The Anthem data breach could harm a record number of victims. If you stay vigilant and follow the steps outlined above, you can keep your finances, your insurance, and your bank accounts safe.

Topics: Identity

Subscribe to Email Updates