FEDERAL TRADE COMMISSION
CONSUMER INFORMATION

consumer.ftc.gov

Anthem Hack Attack, Part 2: Phishing Scams

February 10, 2015
by Colleen Tressler
Consumer Education Specialist, FTC

Last week I told you about health insurer Anthem's data breach affecting more than 80 million customers. This week, I'm telling you about scam artists who are sending phony "Anthem" emails that pretend to help customers, but actually phish for their personal information.

The phony email is designed to look as if it comes from Anthem and asks customers to click on a link for free credit monitoring or "credit card account protection." Don't let that fool you. Anthem says it will contact current and former customers by postal mail with specific information on how to enroll in credit monitoring. Anthem also says it's not calling customers about the data breach or asking for credit card information or Social Security numbers over the phone.

So, if you get an email that says it's from Anthem offering you services in response to the data breach, **don't** reply, click on any links, or open any attachments. Instead, forward it to the Federal Trade Commission at spam@uce.gov, and delete the message from your inbox. To learn more, read our article on how to deal with phishing scams.

Blog Topics: Privacy & Identity