

# NEWS BRIEF

## Important Update from Anthem Regarding the Cyber Attack

Members who may have been impacted by the cyber attack against Anthem should be aware of scam email campaigns targeting current and former members. These scams, designed to capture personal information (known as “phishing”) are designed to appear as if they are from Anthem and the emails include a “click here” link for credit monitoring. Anthem DID NOT send these emails.

- **DO NOT click on any links in email.**
- **DO NOT reply to the email or reach out to the senders in any way.**
- **DO NOT supply any information on the website that may open, if you clicked on a link in email.**
- **DO NOT open any attachments that arrive with email.**

Anthem is **not** calling members regarding the cyber attack and are not asking for credit card information or social security numbers over the phone.

This outreach is from scam artists who are trying to trick consumers into sharing personal data. There is no indication that the scam email campaigns are being conducted by those that committed the cyber attack, or that the information accessed in the attack is being used by the scammers.

Anthem will contact current and former members via mail delivered by the U.S. Postal Service about the cyber attack with specific information on how to enroll in credit monitoring. Anthem will individually notify current and former members whose information has been accessed. Anthem will provide credit monitoring and identity protection services free of charge so that those who have been affected can have peace of mind. Anthem has created a dedicated website ([www.AnthemFacts.com](http://www.AnthemFacts.com)) where members can access information such as frequently asked questions and answers. Anthem have also established a dedicated toll-free number that both current and former members can call if they have questions related to this incident. That number is: 1-877-263-7995.

For more guidance on recognizing scam email, please visit the FTC website: <http://www.consumer.ftc.gov/articles/0003-phishing>.



Be ready for anything.®