Blackbaud Incident Notification 2020

Maintaining transparency and confidentiality of our generous supporters is a top priority for the ThedaCare Family of Foundations. We recently received communication involving a cyberattack on a third-party computing company, Blackbaud, a system we use to help manage donor information.

What Happened

ThedaCare was recently notified by Blackbaud of a security incident involving nonprofit organizations across the country, including schools and foundations. At this time, we understand Blackbaud discovered and stopped a ransomware attack. After discovering the attempted attack, Blackbaud's Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from fully accessing and encrypting files; and ultimately expelled them from their system. Unfortunately, prior to locking the cybercriminal out, the cybercriminal removed a copy of Blackbaud's backup file containing some personal information.

What Information Was Involved

It is important to note that the cybercriminal **did not** access credit card, banking or social security data. However, we have determined that the file removed may have contained your contact information, and a history of your relationship with the Foundation.

Because protecting customers' data is their top priority, Blackbaud paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed.

Based on the nature of the incident, Blackbaud's research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly.

What Is Blackbaud Doing

Ensuring the safety of your data is of the utmost importance to us. As part of Blackbaud's ongoing efforts to help prevent something like this from happening in the future, they have already implemented several changes that will protect your data from any subsequent incidents.

First, Blackbaud's teams were able to quickly identify the vulnerability associated with this incident, including the tactics used by the cybercriminal, and took swift action to fix it. They have confirmed through testing by multiple third parties, including the appropriate platform vendors, that their fix withstands all known attack tactics. Additionally, they are accelerating efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

What You Can Do

As a best practice, we recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities.

For More Information

We sincerely apologize for this incident and regret any inconvenience it may cause. Should you have any questions or concerns regarding this matter, please do not hesitate to contact Courtney Weiland, Vice President of Philanthropy, at Courtney.Weiland@thedacare.org or by phone at (920) 738-6503.