What is a Critical Threat Notification?

SecureSurf™ works around the clock to shield your network from all known and suspected malware types that are found in every corner of the internet. But SecureSurf now monitors your network from within to ensure that any malware that's already in your system isn't trying to send information back to its creator. If SecureSurf detects malware attempting to send out information, it will generate a Critical Threat Notification and send it to everyone in your notification list. A few of the more common questions about this feature are answered below:

Why have I received a notification?

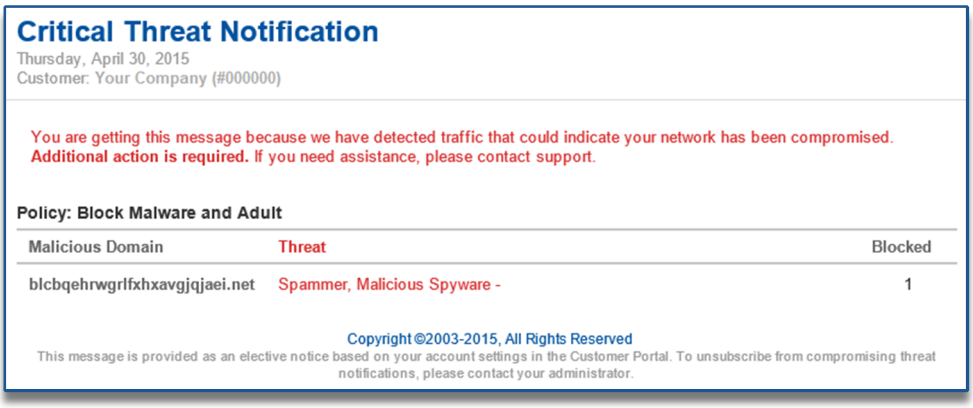
To start, you have been notified because you were listed as a point-of-contact to receive notifications if SecureSurf detects web traffic that indicates your network has been exposed to possible malware.

What exactly does it mean for my network?

Designed as an early-warning detection initiative, the notification indicates that SecureSurf has identified a Botnet, Key Logger or other malicious program that is attempting to send out information from within your network. In other cases, one of the browsers on your network may have been blocked from reaching a site that contains malware. The notification will list the malicious domain, threat type and the number of times the threat has been blocked prior to the notification. This information gives you a head-start in tracking down potential weaknesses or dangerous activity on your network.

By logging DNS requests for your network, administrators can often isolate a suspected workstation or server that may have been compromised due to malware activity. For more information on enabling DNS Request logging for your Windows Server, please visit the following article:

https://support.appriver.com/kb/a669/enable-dns-request-logging-for-windows-2003-and-above.aspx



Critical Threat Notification

Thursday, April 30, 2015
Customer: Your Company (#000000)

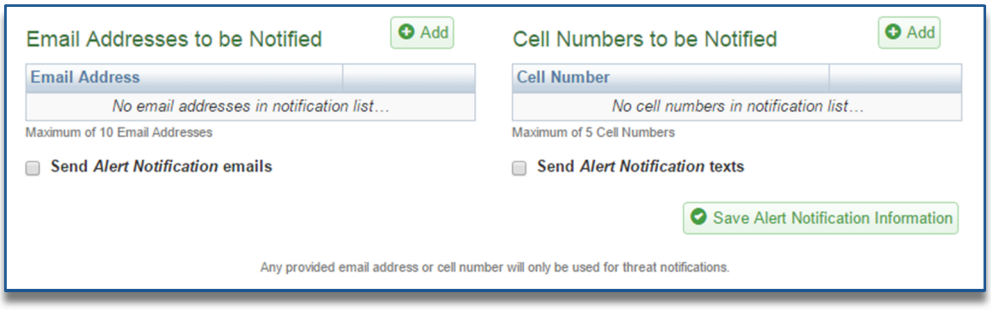
You are getting this message because we have detected traffic that could indicate your network has been compromised. **Additional action is required.** If you need assistance, please contact support.

Policy: Block Malware and Adult

Malicious Domain	Threat	Blocked
blcbqehrwgrlfxhxavgjqjaei.net	Spammer, Malicious Spyware -	1

How do I add contacts to the notification list?

Simply login to the Customer Portal as an Administrator, select the Web Protection Admin tab and then select the Alert Notifications page. From there, add a maximum of ten email addresses and up to five cell numbers to each respective list. Then select the appropriate checkbox to enable the notification(s) and click the **Save Alert Notification Information** button to activate threat notifications for your account.



Of course, SecureSurf from AppRiver is backed with Phenomenal Customer Care™, which provides US-based support from our own team of professionals 24 hours a day, every day. Simply call us toll-free at (866) 223-4645 or e-mail us at support@appriver.com to discuss your Critical Threat Notifications, or anything else. We look forward to hearing from you.