Norton Web Safe Erroneously Blocks Metro Seniors Website and Posts

My Norton product incorrectly alerts that a file is infected, or a program or website is suspicious

A false positive occurs when your Norton product incorrectly alerts that a file is infected, or a program or website is suspicious. Common indicators of a false positive are:

- Your Norton product detects a threat in a file that you believe is unlikely to be infected (for example, files with extensions such as, *.txt, *.dbf, *.log, *.hlp).
- Your Norton product alerts that a file or program developed and created by you or a legitimate company is suspicious, or is a threat
- Your Norton product indicates that a legitimate website is malicious
- Your Norton product blocks downloading a file as suspicious

Metro Seniors website and posts generate many posts with lots of media files (doc, pdf, txt, xls, and so on) to give members detailed information on tournament results, pace of play, rules, and ,much more. In addition, we have several contributors who post and revise data and media files.

Recently, we had a post with minor errors that was deleted immediately after publication and email was sent to subscribers. The link in the post was missing, and this broken link immediately generated warnings and blocks for at least some of our members who use Norton Web Safe.

Norton will evaluate and re-rank a site if:

1. Site purchases a site maintenance subscription (essentially extortion)
2. If site owner certifies that site is not malicious (on their own priority and schedule – days/weeks)
3. If Norton Web Safe users (you) report the warnings and blocks as false.

We are NOT planning to purchase a site evaluation subscription from Norton. We already have several security systems purchased and in use through our web site host.

I will contact Norton as site owner, but this is difficult, and not timely.

If you are a Norton Web Safe user, I ask that you immediately report to Norton these as “false positives” per their procedure below.

How to report a false positive?

- Before submitting a false positive, make sure that your Norton product has the latest definition updates. Run LiveUpdate to install all the available updates for your Norton product and then run a Full system scan.

If the false positive still occurs with the latest definitions, report it to Symantec. The link to submit a false positive differs based on the exact detection, or the alert you receive.

Report a Suspected Erroneous Detection (False Positive)

Report a Suspected Erroneous Detection (False Positive)

Use this "wizard" to tell us about a situation where you believe that a Symantec or Norton product is incorrectly reporting a clean / good file or website as being a threat or malicious in some way. This is sometimes called a False Positive. Your answers to these three or four questions will help us get your report to the correct internal team to quickly review your report.

Please ensure you have read the following guidelines before making a submission
• Click here for SEP product guidelines.
• Click here for Norton product guidelines.
• Click here for Symantec Advanced Threat Protection product guidelines.

When did the detection you are reporting occur?

- ○ A1 - When downloading or uploading a file
- ○ A2 - While using an application
- ○ A3 - When installing an application
- ○ A4 - When browsing the web
- ○ A5 - During a scheduled scan, or during a scan I requested
- ○ A6 - When sending or receiving email
- ○ A7 - While writing or reading files to/from a storage device
- ○ A8 - Don't know, am unsure, or the options provided do not apply

Next »

I am a Symantec Endpoint Protection 12.1 user and want to exclude a detection »

I have a question about the stability rating of an application »

I am a Symantec Advanced Threat Protection user and want to whitelist a file or domain. »

What to do after you submit a false positive?

After submitting the file, wait until you receive the confirmation email from Symantec. In the mean time, you can try updating the definitions and scan the incorrectly detected file or application at frequent intervals.

Perform the following steps only if your business is getting impacted, or if you are certain that the file is safe, or if you are a developer who created the file.

Turn off Download Intelligence

1. Start your Norton product.

2. Click **Settings**.
3. Under **Detailed Settings**, click **Firewall**.
4. On the **Intrusion and Browser Protection** tab, next to **Download Intelligence**, click on the slider to turn it **Off**.
5. Click **Apply**.
6. In the **Security Request** dialog box, in the **Select the duration** drop-down list, select the duration that you want to turn off Download Insight for, and then click **OK**.
7. Click **Close**.

   If you are certain that the file is good, then you can exclude the files or folders from being scanned.

Exclude files or folders from scan

If you are certain that the file is good, then you can exclude the files or folders from being scanned.

1. Start your Norton product.
2. Click **Settings**.
3. Under **Detailed Settings**, click **Antivirus**.
4. On the **Scans and Risks** tab, scroll down to **Exclusions / Low Risks**.
5. Next to **Items to Exclude from Auto-Protect, SONAR and Download Intelligence Detection** row, click **Configure**.
6. In the **Real Time Exclusions** window, click **Add Folders** or **Add Files**.
7. Browse for and select the folders or files that you want to exclude from the scan, and then click **OK**.
8. Click **Apply**, and then click **OK**.