How do I use the Website Malware Scanner?

Site Management · https://computancy.co.uk/kb/how-do-i-use-the-website-malware-scanner/

Overview

One of the major problems with malware is its persistence. This is why computancy's Website Malware Scanner makes daily scans of all the sites within your hosting account. It uses a combination of commercial and in-house tools and provides reports detailing identified malicious content and its location within your site files.

When malware is located on a site, PHP mail is automatically disabled. We do this to preserve sender reputation across the platform and ensure that any sites that are compromised do not send large volumes of spam emails.

Best practices when dealing with malware and infected files

- Check the Malware Report produced by the malware scanner to identify if there are any infected files
- Clean and remove the infected files from your webspace
- Identify any vulnerabilities within the site and secure them

Taking regular backups means that you'll always have a restore point if you do find your site with compromised files.

Checking the Malware Report

The Malware Scanner shows you a full list of sites that are currently infected within your account. To access this list:

- Login to https://clients.computancy.uk
- Select the **Malware Report** icon.
- If any sites are currently infected they will show up here.

It shows: the package where the infection has been found, the time of the last scan and the number of infected files. To show a more detailed report, select **View Report**. You will now see

the full list of infected files on the site.

Infections found marked in red indicate that the file could be a risk to the site.

We also have a yellow ‘warning’ state which shows that the signatures found are unlikely to pose a high risk to the site. For example: logs files, SQL files and .zip backups files. Essentially a yellow warning state is for ‘information-only’ and won’t impact the sending of mail.

You can ensure that you're notified of any newly-discovered malware by checking the **Receive Daily Email Alerts?** box.

Cleaning and removing infected files

In most cases the best way to resolve an issue with malicious content is to remove the compromised files and replace them with versions from a known clean download. That is, download the software again and replace just the files that have been infected from the initial install.

If the files are not needed, then you could also just delete the files completely.

Sometimes an infected file will just have the attackers script 'injected' in the first or last line within a specific file. Sometimes this can be very obvious, in which case you could look to simply remove the malicious script.

You’ll want to do this for all the files that have been found by the Malware Scanner.

Further actions you can take

Remove unnecessary or unused plugins and applications from the site. Doing this will not only reduce the number of potential vulnerabilities but also make general site 'house-keeping' simpler.

You should also make sure that any plugins you're using are always kept fully updated. Outdated software versions are much more likely to have security vulnerabilities - leading to compromised sites.

Change passwords such as your database password and FTP password.

Note: Don’t forget to update any configuration files such as wp-config.php after making the changes.

Rescanning the site

You can re-scan the site on demand. Once you believe you've removed the malware, head back to the Malware Scanner and select 'Scan Again'.

If all infected files are removed, then PHP mail will automatically be re-enabled and there will be no infected files displayed. The scanner will continue to take daily scans of all your sites to ensure you're always aware of any sites that have been compromised.