Reputation

Hatred or Violence

Browser plug-ins like WOT [1] allow to evaluate a website by the user, e.g.regarding questionable contents like hate speech, racism or discrimination. Your website has received poor ratings in this category. The result is that the plug-in warns users about a possible danger when visiting your website. This can lead to a damage of your reputation.

Solution

Monitor your users' behaviour and try to find the reason for the poor evaluation. If you suspect that your website has been rated bad unjustified by the intention to harm your reputation, you have the possibility to contact the plug-in developers [2].

- [1] https://www.mywot.com/
- [2] https://www.mywot.com/en/support/feedback

Misleading

Browser plug-ins like WOT [1] allow to evaluate a website by the user, e.g. point out misleading, incorrect or unethical content or unproven product claims. Your website has received poor ratings in this category. The result is that the plug-in warns users about a possible danger when visiting your website. This can lead to a damage of your reputation.

Solution

Monitor your users' behaviour and try to find the reason for the poor evaluation. If you suspect that your website has been rated bad unjustified by the intention to harm your reputation, you have the possibility to contact the plug-in developers [2].

- [1] https://www.mywot.com/

- [2] https://www.mywot.com/en/support/feedback

Adware

Browser plug-ins like WOT [1] allow to evaluate a website by the user, e.g.regarding unwanted advertisements like highly annoying ads and pop-ups. Your website has received poor ratings in this category. The result is that the plug-in warns users about a possible danger when visiting your website. This can lead to a damage of your reputation.

Solution

Monitor your users' behaviour and try to find the reason for the poor evaluation. If you suspect that your website has been rated bad unjustified by the intention to harm your reputation, you have the possibility to contact the plug-in developers [2].

- [1] https://www.mywot.com/
- [2] https://www.mywot.com/en/support/feedback

Experience

Browser plug-ins like WOT [1] allow to evaluate a website by the user, e.g. user experience regarding unacceptable user experience, low quality products or unreliable deliveries. Your website has received poor ratings in this category. The result is that the plug-in warns users about a possible danger when visiting your website. This can lead to a damage of your reputation.

Solution

Monitor your users' behaviour and try to find the reason for the poor evaluation. If you suspect that your website has been rated bad unjustified by the intention to harm your reputation, you have the possibility to contact the plug-in developers [2].

- [1] https://www.mywot.com/
- [2] https://www.mywot.com/en/support/feedback

Scam

Your website has been blacklisted as it has been identified as fraud. This might indicate that your website has been hacked and third parties may have access to your system. This means that your website may harm users by phishing attacks and scam which can have a negative impact on your reputation.

Solution

Carry out an anti virus scan immediately and contact your web hosting provider to inform him about you being hacked. Furthermore, please check the following information that may help you to resolve this issue [1]. If you suffer from hacking attacks frequently or if the problem persists even after the recovery we strongly recommend to consult an IT security expert to help you.

- [1] https://developers.google.com/search/docs/advanced/security/overview

Illegal

Your website has been blacklisted as it has been identified to hosting malicious or illegal content. This might indicate that your website has been hacked and third parties may have access to your system. In Addition to a severe damage of your reputation, hosting illegal and malicious content may have legal consequences for you.

Solution

Carry out an anti virus scan immediately and contact your web hosting provider to inform him about you being hacked. Furthermore, please check the following information that may help you to resolve this issue [1]. If you suffer from hacking attacks frequently or if the problem persists even after the recovery we strongly recommend to consult an IT security expert to help you.

- [1] https://developers.google.com/search/docs/advanced/security/overview

Potentially Unwanted Application (PUA)

Browser plug-ins like WOT [1] allow to evaluate a website by the user, e.g. if the site installs or is involved in the distribution of potentially unwanted programs or applications (PUA) like toolbars without notifying the user. Your website has received poor ratings in this category. The result is

that the plug-in warns users about a possible danger when visiting your website. This can lead to a damage of your reputation.

Solution

Monitor your users' behaviour and try to find the reason for the poor evaluation. If you suspect that your website has been rated bad unjustified by the intention to harm your reputation, you have the possibility to contact the plug-in developers [2].

- [1] https://www.mywot.com/
- [2] https://www.mywot.com/en/support/feedback

SPAM

Your website has been blacklisted as it has been identified to send spam. This might indicate that your website has been hacked and third parties may have access to your system. Furthermore, this can refer to insecure configuration of a mail server which is used as an open relay. Another reason for blacklisting can be poor user evaluation via browser plugins such as the WOT Add-on [1] which allows users to tag websites if they are used to sending spam or if they are referred to in spam mails.

The consequence is, additionally to a great loss of reputation, impairment of the e-mail traffic on the system as mails are marked as spam mails.

Solution

Try to figure out the reason why your website has been blacklisted. Check if your system can be used as an open relay and secure your system's configuration [2]. Moreover, it is recommended to carry out an anti virus scan and to contact your web hosting provider to inform him about your problem. If the problem was due to malicious software, please check the following information that may help you to resolve this issue [3].

If you managed to solve the underlying problem follow the blacklist removal process of the specific blacklist provider.

If you suffer from being blacklisted frequently or if the problem persists even after fixing your configuration issues we strongly recommend to consult an IT security expert to help you.

- [1] https://www.mywot.com/
- [2] http://www.mailradar.com/openrelay/

- [3] https://developers.google.com/search/docs/advanced/security/overview

Malware

Your website has been blacklisted as it has been identified to hosting malicious software. This might indicate that your website has been hacked and third parties may have access to your system. This means that your website may harm users which can have a negative impact on your reputation.

Solution

Carry out an anti virus scan immediately and contact your web hosting provider to inform him about you being hacked. Furthermore, please check the following information that may help you to resolve this issue [1]. If you suffer from hacking attacks frequently or if the problem persists even after the recovery we strongly recommend to consult an IT security expert to help you.

- [1] https://developers.google.com/search/docs/advanced/security/overview

Reputation

Browser plug-ins like WOT [1] allow to evaluate a website by the user regarding several categories. Your website has received general poor ratings by them indicating a bad reputation. The result is that the plug-in warns users about a possible danger when visiting your website.

Solution

Monitor your users’ behaviour and try to find the reason for the poor evaluation. If you suspect that your website has been rated bad unjustified by the intention to harm your reputation, you have the possibility to contact the plug-in developers [2].

- [1] https://www.mywot.com/
- [2] https://www.mywot.com/en/support/feedback

Suspicious Links

The domain of an outgoing link found on your website is on a blacklist. There are two possible causes. Either your website has been hacked, and someone placed malicious links on your website, or the legit website you are linking to has been hacked and was indentified by a blacklist. Both can cause an immediate reputation loss, because search engines use outgoing links in their ranking calculation.

Solution

Review the links. If they lead to legit websites, inform the owner of that website about the blacklist listing. If they lead to unknown/malicious websites delete them and take further actions to resecure your website. Please check the following information that may help you to resolve this issue [1]. If you suffer from hacking attacks frequently or if the problem persists even after the recovery we strongly recommend to consult an IT security expert to help you.

- [1] https://developers.google.com/search/docs/advanced/security/overview

Phishing

Your website has been blacklisted as it has been identified as phishing site. This might indicate that your website has been hacked and third parties may have access to your system. Your website may be misused, by masquerading as a trustworthy entity to obtain sensitive information from your users.

Solution

Please check the following information that may help you to resolve this issue [1]. If you suffer from hacking attacks frequently or if the problem persists even after the recovery we strongly recommend to consult an IT security expert to help you.

- [1] https://developers.google.com/search/docs/advanced/security/overview

---

Revision #1
Created 2 August 2021 06:43:18 by Patrick Wall
Updated 2 August 2021 07:26:23 by Patrick Wall