What is a Deface attack? How to prevent Deface attacks

Deface attacks are attacks that change the visual appearance of a website. This is often the action of hackers who specialize in hacking systems. They break into a web server and replace the hosted website with their own website.

People always focus on protecting data. Phishing, Social Engineering and cyber attacks such as DDoS keep companies on guard against suspicious behavior. However, there is an even greater threat to society. That is the website Deface attack. Deface a website can cause global panic within minutes.

What is a Deface attack?

Deface attacks are attacks that change the visual appearance of a website. This is often the action of hackers who specialize in hacking systems. They break into a web server and replace the hosted website with their own website.

The most common Deface attack is to use SQL Injection to log into the admin account. Usually the website Deface attacker will point out a flaw in maintaining the system administrator's server security. In most cases, these attacks are harmless. However, they can be used as a distraction to cover up other malicious behaviors, such as uploading malware or deleting necessary files from the server.

Deface attack

How to prevent Deface attacks

To gain access to your site, cybercriminals often visit contact forms, spam comments, insert unwanted links into source code or databases. The more entry points your site has, the easier it will be for an attacker to gain access. Follow these tips to prevent cyber criminals from attacking and keeping your site protected:

1. Cybercriminals often target websites that are considered vulnerable or will attract a lot of attention if hacked. Typically, websites that are particularly vulnerable are those that incorporate many plugins and extras. Research shows that WordPress websites with 6 to 10 plugins are twice as likely to be hacked than sites without plugins. Basically, add-ons expand the website surface, giving hackers more potential entry points.

One way to prevent a Deface attack is to **choose your plugins and applications very carefully** . Make sure each plugin is valid for the website and only uses what you need. Regularly check add-ons and completely uninstall any plugins or themes that have been deactivated in the dashboard.

Unused add-ons may be outdated and become less secure over time, leaving your site vulnerable to attack. Outdated software is a leading factor in cyber attacks, because the code is not updated, so it is very vulnerable. You should also **update important plugins, themes, and files as soon as an update is available** .

2. **Restrict access level** . If more people log in to the site to change the content, limit the type of access that each individual has. Having multiple admins on the site will open the door for cybercriminals to gain unauthorized access via the login page. Restricting full access to content can prevent the website Deface attack due to human error (for example, weak passwords).

Protect the website

3. **Scan the website source** . If you have a technical background or tech-savvy staff, you can test your site for malware yourself. You should also have access to the file manager provided by the domain host or file transfer protocol, both of which can be used to check websites and look for malware.

You finished reading the article "**What is a Deface attack? How to prevent Deface attacks**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.