Don't ignore these 10 security tips when creating a new website

When setting up a new website, it is important to make sure that the site is safe. Fortunately, most things you need to do are very easy. Some security tips will take a little time, but it is a worthy 'investment'. Do not let your site unprotected!

When setting up a new website, it is important to make sure that the site is safe. Fortunately, most things you need to do are very easy. Some security tips will take a little time, but it is a worthy 'investment'. Do not let your site unprotected!

1. Design website with Adobe Dreamweaver CS5 software - Part 1

1. Choose a secure domain name provider

When registering a domain name for your website, you need to ensure that no one can control it. If a fraudster can log your domain name, they can turn it into theirs or sabotage the site.

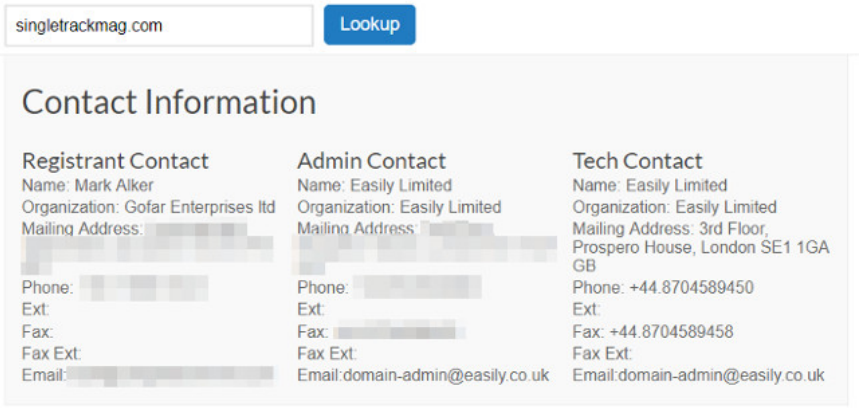
There are several domain provider options that use two-factor authentication (2FA). This adds to the level of security and makes access much more difficult. Even if someone has a password, they need to access your phone.

Here are some domain providers that authenticate two factors: Dynadot, GoDaddy, Lexsynergy, Name.com, NameCheap.

2. Hide your information from WHOIS

Every website has a WHOIS section and if you don't take steps to ensure that your information is protected, your name and email address will be easily found by spam companies. Both your name and email address are necessary information for identity theft, so keeping this information safe is necessary.

1. How to search for free online resume



Most web hosts offer anonymous WHOIS registration for a small fee, but there are also a few that offer free registration. Both Dreamhost and 1and1 allow you to open a website with anonymous WHOIS information without losing a fee.

Whether you decide to pay or use it for free, do what you need to keep your name and email from appearing in your WHOIS profile. It will save you time to deal with a lot of spam and make it harder for people who want to get your information.

3. Change the password

If the domain name, host, CMS or anything else comes with a standard administrator password, change the password now. You even have to change your username from "admin" to something else if it's the default.

Changing passwords often is not a bad idea. Use the password manager to track them and make sure they are secure.

4. Update software for the website

Once you've secured the registration, it's time to secure the site. And the first step, like the first step to ensure anything else is keeping everything up to date.

When companies discover vulnerabilities in security, they will release patches and updates. If you do not update your software, you will be vulnerable to "loss". Most hosts will prompt you to update when there is a new version. However, you should regularly check your version information.

5. Use safe plugins

If you are using a content management system (CMS), there are secure plugins available. Big names like WordPress, Drupal, Joomla and Magento all have a lot of plugins. All you need to do is choose the most suitable ones, then download, install and activate.

Each CMS and security extension will give you advice on exactly what you should use. You should also consult third-party reviews about secure plugins. But if the plugin is of a reputable provider, it will help keep your site safe. Use advanced security settings to remove security holes and keep your extension up to date.

6. Turn on HTTPS

This is not just your own security as you think. Both visitors and Google will appreciate that you have encrypted all the traffic on your site. Especially if visitors share any sensitive information.

Some hosting services automatically enable HTTPS for you and others allow you to do that with a few simple steps. If you are hosting or renting a web server yourself, enabling HTTPS will be more difficult because it involves buying an SSL certificate, enabling it and configuring your site to use HTTPS.

1. What is SSL? Is SSL important to the website?

It is not too complicated, but the process may be different on your hosting service, so check the service and find the best way to do this.

7. Check access

Different users on your site will have different access rights. As an administrator, you have the right to change anything you want, others will be more limited. CMS often allows you to change permissions for regular visitors, logged in, edited, contributors and many other user groups.

Think about how much access each group has. Do your editors need to create new users? Can your readers edit the page? Give each person the minimum rights to perform their work.

You can use an FTP client to view all files on your site and check permissions with symbolic or numeric symbols. You can then use the commands to change permissions.

8. Hide admin page

The websites you use to log in and manage should not be displayed on search engines. This may not be like a security measure, but it will make it harder for those who intend to find those sites for malicious purposes. It is easy to hide the admin page, only takes a few minutes.

Some CMS and security plugins will allow you to hide these pages from search engines. If your device does not provide this functionality, you can do it manually by editing the robots.txt file, which is accessible from the CMS installation or the cPanel administrator section. Add the following lines to the file:

*User-agent: **

Disallow: [the relative URL of the page]

In WordPress, you will use '/ wp-admin /' as the URL. Other CMSs will have different URLs. You may also not allow users to view any other pages. This not only ensures the security of the website but also helps optimize your search engine.

9. Protection against security vulnerabilities Scripting Cross-Site (XSS)

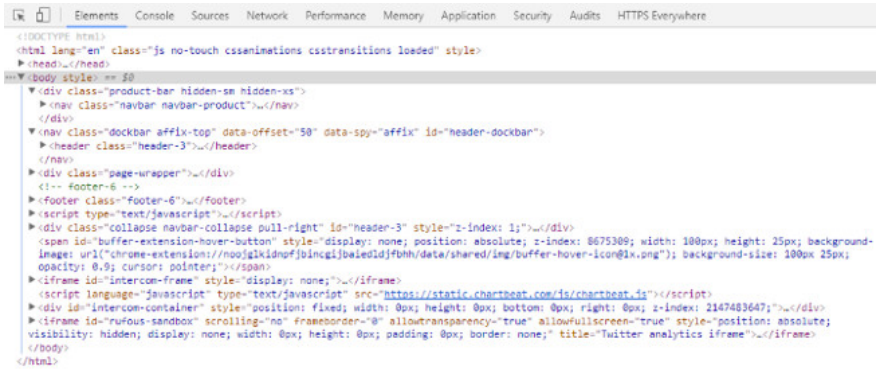
XSS is a hack trick that involves running code on your website. For example, it can happen in a contact form that includes a script in it, a hacker can make your site execute that code, allowing them to access or cause destruction to the site. yours.

Protection against this type of attack is actually quite complicated. If you want to learn about the methods you can use, try the excellent anti-XSS cheat sheet from OWASP. If you don't know much about technology, there are many XSS anti-plugins available, some standard security plugins can handle this security hole. However, make sure your site is protected.

10. Prevent information leakage

While XSS, SQL injection, password cracking and other hacking methods may seem the most dangerous, it is impossible to ignore the simplest things as it can cause problems. Information leakage is one of those things.

When you accidentally give information that you don't intend (or don't know), it's information leakage. It's easy for developers to accidentally leave HTML comments in your website code.



If you are using with a standard CMS, this will not be a big problem. But if you have asked or hired someone to design a custom theme, you should check the leak information. One of the best ways is to just use the **View Source** option in your browser and quickly scan the HTML comments that are not deleted.

Larger sites that include hundreds or thousands of pages may require a security specialist (or at least a trainee) to check this section. Either way, this is an easy way to check, so don't skip this step.

Protect your website now!

When creating a new website, there is a lot of work you have to do. And it's easy to forget these basic security measures. But these measures can help you solve many long-term problems. So don't ignore them! Make sure your site is secure before you start creating content.

You finished reading the article "**Don't ignore these 10 security tips when creating a new website**" 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.