

In order to protect your website from hackers, your web hosting company provides a wide variety of security measures. You play the most important role in protecting your site. For increased site security, follows these practices.

Utilize Firewalls

In order to prevent unauthorized entries into a computer server, most servers have firewalls, which block packets of bad information from infiltrating a server. If you are unsure how to configure a firewall, your hosting provider can usually provide additional security measures. Some corporate website owners decide to purchase separate servers from their web hosting company, in order to provide additional firewall measures.

Use Difficult Passwords

In order to gain access to website data, computer hackers frequently use brute force hacking, which attempts millions of different character combinations. When choosing a website password, use both lower and upper case letters, as well as a number and a symbol. Make sure your password at least 10 characters long.

Check Server System Logs

When attempting to break into your website, hackers often leave an electronic trail. Check your raw server logs, in order to locate repeated hits from suspicious IP addresses. Report this activity to your web host administrator. Oftentimes, hackers require multiple attempts to break into a web server, so monitor your log activity on a daily basis.

Update Your Blog Software

Operating system vendors release frequent server security patches. Your web hosting provider will install many of these updates for you. If you use Wordpress, or a similar blog platform, always update your installation. When it is time to upgrade your Wordpress installation, a yellow warning bar will show up at the top of the screen.

Limit Access

When you are blogging, do not give out your administrator password. For multiple users, Wordpress offers different levels of security access. Issue unique passwords to all users. Only assign them the highest priority necessary.

Backup Your Data

After working for hours on a commercial website, you could lose all of your data. Create backups of all of your website files. In the event of failure, your web host provider will provide backups of their own servers, but you should still backup your files regularly, as an extra safety precaution.

Protect Your Computer from Malware

In an attempt to gain access to your site, a determined hacker may manage to sneak a virus onto your computer, known as a key logger, which will record your website password. Run spyware removal programs on a weekly basis, in order to ensure that your computer does not become infected. Free spyware removal programs include Spybot Search & Destroy, Avast!, and Lavasoft Ad-Aware.

Change Your Passwords Regularly

Even with all of these security measures, your password may still be comprised. In order to thwart hacker attempts, change your website password on a monthly basis.

In order to make sure that your website is fully secured, your web hosting provider offers many security features with their hosting service, but it is important to do your part.