

Web site security has become something to definitely be concerned about. There are people and companies out there that thrive on snooping into web sites. We all need to do what we can to help curb this disturbing fact.

Our hosting accounts use a VPS Server (Virtual Private Server) which simply means it's much more secure than shared hosting. VPS is just one step away from a dedicated server which in most cases is not necessary and for which you pay dearly! Dedicated servers are those that are used by banks and other financial institutions.

Most web sites do not need a dedicated server host. The security measures in place on our VPS server itself and some additional precautionary measures taken by you and your web designer are generally sufficient to protect your web site.

What and What Not To Do

Never ever give out login information of any kind to someone you do not trust. Of course, these days it comes down to "who can you really trust?" Definitely something to think about!

Make sure to follow your web designer's suggestions should there be a need for additional security for your web site. If you're not sure, ask!

Check your web site on some kind of regular basis. This doesn't mean just the home page either! A web site shouldn't work like the cruise control in your car — you don't just "set it and forget it!"

If you find any unauthorized changes or something just "doesn't seem right" contact your designer immediately and let them know. If you feel you should contact your designer, they need a place to begin tracking down the problem. You will be a huge help with this by providing them with very specific information which will aid in finding and fixing the problem as quickly and cost effectively as possible. **Always** include the following information:

- Be specific in describing what you see.
- Provide a link to the page in question.
- Provide your browser name & version.
- Tell them why you're concerned.

Providing the above information gives your web designer a starting place to investigate. If you don't give them this information, they're only going to have to ask you for it anyway, which will delay any possible fix that may be needed.

Unless your design or maintenance contract specifically states that your site is being regularly monitored for security issues, don't expect nor assume that your web designer is doing so! This is not a normal every day service provided by web designers! Your web site is your responsibility in this respect. If we had to continuously check every client's web site, we would never get any work done for you or anyone else!

Additional Security Measures

Use an .htaccess file to redirect any potentially unsecure links or url's that a visitor (hacker)

could type into the address bar of your browser.

Examples:

Redirect permanent /pagename.html https://www.sitename.com/~login
name/secure/pagename.html

Redirect permanent /secure/pagename.html https://www.sitename.com/~login
name/secure/pagename.html

The above lines need to be each on their own separate line with no breaks in them. Note the "s" in the http ... this indicates the page(s) are stored in a secure folder of the web site.

What will happen is that the user who happens upon a non-secure link to the secured page on your site will automatically be redirected to the secure page without even noticing.

Here is another trick to help keep things secure and this applies to any site, not just a site that has a secure page(s). If a visitor types in a url for a domain that doesn't use an index page say in a sub-folder ...

Example:

http://www.sitename.com/images/

Yikes! Snoopers get a link-clickable list of every file in that folder! You may as well have handed to them on a silver platter!

The following line added to the .htaccess file will cure this!

```
IndexIgnore */ *
```

This one line in the .htaccess file takes care of every sub-directory in the site!