







Suggested content for .htaccess files in folders where there is an index.html file but not yet an .htaccess file would be something like the following (depends on your server configuration):

```
#.htaccess to prevent unauthorized directory browsing or access to .php files
IndexIgnore */*
<Files *.php>
  Order Deny,Allow
  Deny from all
</Files>

#add the following to protect against people discovering what version your spiders.txt file is
<Files *.txt>
  Order Deny,Allow
  Deny from all
</Files>
```

If your webhost configuration doesn't allow you to create/use your own .htaccess files, sometimes they provide an interface in your hosting admin control panel where you can set the desired .htaccess settings.

It is recommended that you work with your host to configure these settings if this is the method they require. You need to choose, and use, the appropriate method for your server. As mentioned above, it's best to work with your web hosting company to select and implement the best method for your specific server. We can't tell you what to use for your specific server, but we offer these guidelines as a starting point.

### h3. 9. Disable "Allow Guest To Tell A Friend" feature

You may wish to go to Admin > Configuration > Email Options > Allow Guest To Tell A Friend and set the option to false. This will prevent non-logged-in customers from using your server to send unwanted email messages.

### h3. 10. Protect your "images" and other folders

During initial installation, you are advised to set your images folder to read/write, so that you can use the Admin interface to upload product/category images without having to use FTP for each one. Similar recommendations are made to other files for various reasons.

However, leaving the images (or any other) folder in read/write mode means that hackers might be able to put malicious files in this (or other) folder(s) and thus create access points from which to attempt nasty exploits.

Thus, once your site is built and your images have been created/loaded, you should drop the security down from read/write to read. ie: change from CHMOD 777 down to 644 for files and 755 for folders.

#### File/Folder permissions settings

On Linux/Unix hosts, generally, permission-setting recommendations for basic security are:

- \* folders/directories: 755
- \* files: 644

On Windows hosts, setting files read-only is usually sufficient. Should double-check that the Internet Guest Account has limited (read-only) access.

## Folder Purposes

The folders for which installation suggests read-write access for setup are these. If your site supports .htaccess protection, then you should use it for these folders.

### \* /cache

This is used to cache session and database information. The BEST security protection for this is to move it to a folder "above" the public\_html/htdocs/www area, so that it's not accessible via a browser. (Requires changes to DIR\_FS\_SQL\_CACHE setting in configure.php files as well as Admin > Configuration > Sessions > Session Directory.

### \* /images

See other suggestions earlier.

### \* /includes/languages/english/html\_includes

See other suggestions earlier.

### \* /media

This is only suggested read-write for the sake of being able to upload music-product media files via the admin. Could be done by FTP as an alternative.

### \* /pub

This is used on Linux/Unix hosts to have downloadable products made available to customers via a secure delivery method which doesn't disclose the 'real' location of files/data on your server (so that people can't share a URL and have their friends steal downloads from your site)

### \* /admin/backups

This is used by automated backup routines to store database backups. Optional.

### \* /admin/images/graphs

This is used by the Admin > Tools > Banner Manager for updating/displaying bar graphs related to banner usage. If not writable, feature is ignored.

## Additional Security for Folders having 777 permissions:

For any directory that requires permissions of 777 or, for their own reasons, one wants to have permission of 777 the following should be put within an .htaccess file used for that directory.

```
# This code is great for directories where "NO" script should be run from
# but for whatever reason, you need Directory permissions to be 777 - which is wide-open and insecure by itself.
# Examples Directories would include: any 'images' dir., the 'bmz' dir. if using ImageHandler 2, the html_includes languages folder, etc

# Prevent directory viewing and the ability of any scripts to run.
# No type of script, be it PHP, PERL or whatever can normally be executed if ExecCGI is disabled.
OPTIONS -Indexes -ExecCGI
```

## h3. 11. Remove the print URL feature from your browser

To stop the browser from printing a URL on the invoice or any other document on the web, follow these steps:.

### \* For Microsoft Internet Explorer

- o Click on File then Page Setup
- o At page setup, remove this two character combination "&u" from the header or footer text box.

### \* For Firefox

- o Click on File then Page Setup
- o On the "Margins & Header/Footer" tab, remove all references to "Title" and "URL".

### h3. 12. Things to Check Up on Regularly

1. Be sure you've done all the steps listed in this document
2. Keep good backups of your website files and database
3. Check your server's errorlog regularly for odd or suspicious activity
  - \* look for any links that went to a page that isn't in your site
  - \* look for links that have http after the index.php
4. Check your website files regularly to be sure nothing's been added or altered
5. Ask your webhost what they have done to be sure the server you're on is safe and secure so that outsiders cannot do any harm, and so that other websites on your server cannot be used to get to your site and cause any harm (in case they have security holes in them)
6. If your business warrants, or you still want additional assurance (esp if running forum software on your site, or other scripts outside of Zen Cart), hire a security consultant to check your site regularly and give you peace of mind in exchange for a few dollars