

# SITE SECURITY

USPATENTMENTOR.COM is secured with a Starfield Technologies Web Server Certificate. Transactions on the site are protected with up to 256-bit Secure Sockets Layer encryption.

Domain Control Verified

Starfield Technologies has verified that the certificate holder controls the domain uspatentmentor.com.

Certificate Status valid (06/03/2009 to 06/03/2010).

## ***About Encryption***

WinZip's encryption protects documents contained in your archives from unauthorized viewing.

The contents of the files that you want to protect are encrypted by WinZip® based on a password that we have specified.

**Standard Zip 2.0 encryption:** encryption technique provides a measure of protection against casual users who do not have the password and are trying to determine the contents of the files.

## ***Limitations on Encryption***

Encryption provides a measure of safety for your sensitive documents, but even encrypted documents can be compromised (regardless of encryption software). Here are *some* of the ways this can occur. This is by no means an exhaustive list of potential risks; it is intended only to give you an idea of some of the safety issues involved with sensitive documents.

- If a keystroke monitor or other malicious code (such as a virus) is running on your computer, your password may be recorded when you type it. Be sure to check frequently for viruses and follow other recommended computer safety procedures.
- If you extract an encrypted file and then delete the file, it may be possible for someone to later "undelete" the file using file recovery software or the Recycle Bin.

- When you open or view a file from an archive (e.g., by double clicking it), WinZip must extract the file to a temporary location so that the associated program can open it. If you subsequently close WinZip without first closing the program that is using the file, WinZip may not be able to delete the temporary copy of the file, thereby leaving it on disk in unencrypted form. The associated program may also make one or more backup copies of the decrypted file, and WinZip will not be able to delete these. In addition, as described above, it may be possible for someone to later recover deleted files using file recovery software or the Recycle Bin.
- When you "move" files to a Zip file by choosing the **Move** action in the Add dialog, WinZip moves the files into the Zip file by compressing them and then deleting the original files from the disk. It may be possible to recover the original, unencrypted files from the disk.
- After adding or extracting encrypted files, some or all of the unencrypted file contents may remain in your computer's memory or the page swap files on disk. A malicious user may be able to retrieve this unencrypted information.
- WinZip does not encrypt Zip file comments or, as described above, information about encrypted files such as their names, dates, etc. Any user with access to the Zip file can view this information without a password.

You may be able to eliminate some of these exposures using specialized software such as virus scanners, disk erasers, etc.