How strong is WinZip's encryption?

- WinZip
- WinZip Enterprise
- WinZip SafeMedia
- WinZip Self-Extractor

WinZip offers two kinds of encryption: strong **AES** encryption and weak **Zip 2.0 (Legacy)** encryption.

If you have important security requirements for your data, you should use WinZip's **AES** encryption. AES, the Advanced Encryption Standard, came to be as the result of a three-year competition sponsored by the U.S. Government's National Institute of Standards and Technology (NIST). This encryption method, also known as Rijndael, was adopted by NIST as a Federal Information Processing Standard.

If you have a need for encryption to be FIPS 140-2 compliant, you should consider a WinZip Enterprise license, which has that option.
WinZip supports AES encryption in two different strengths: **128-bit AES** and **256-bit AES**. These numbers refer to the size of the encryption key that is used to encrypt the data. 256-bit AES is stronger than 128-bit AES, but both of them can provide significantly greater security than the standard Zip 2.0 method. A minor advantage of 128-bit AES over the 256-bit AES is that it is slightly faster, that is, it takes less time to encrypt or decrypt a file. This would likely go without notice, unless you were creating Zip files in which you included many thousands of files being encrypted while being added.

The security of your data depends not only on the strength of the encryption method but also on the strength of your **password**, including factors such as length and composition of the password. Security also depends on the measures you take to ensure that your password is not disclosed to unauthorized third parties.

The Zip file format extension used by WinZip to store AES-encrypted files requires WinZip 9.0 or later. Because the full technical specification for WinZip's AES format extension is available on the WinZip web site other Zip file utilities **can add** and **have added** support for this Zip file format extension. In other words, WinZip's AES encryption **is** supported by some other Zip file utilities (but not all).
The **Zip 2.0 (Legacy)** encryption format is supported by nearly all other Zip file utilities. Password protecting a Zip file with Zip 2.0 encryption provides a measure of protection against a *casual* user who does not have the password and is trying to determine the contents of the files. However, the Zip 2.0 encryption format is known to be relatively weak, and cannot be expected to provide protection from individuals with access to specialized password recovery tools.

Note: do not rely on Zip 2.0 encryption to provide strong data security.
