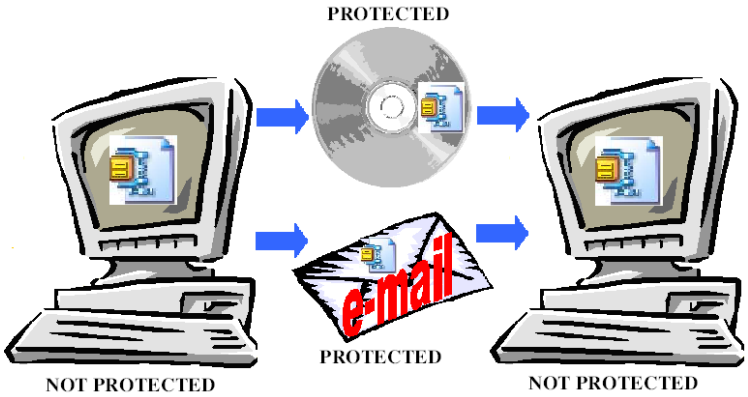
Encrypting Files with WinZip®

WinZip is a popular file compression program for Windows users. WinZip versions 9.0 and higher also offer file encryption with AES using a 128-bit or 256-bit key derived from a user-entered password. An evaluation of file encryption with WinZip versions 10.0 and 11.0 resulted in the recommendations for use listed below.



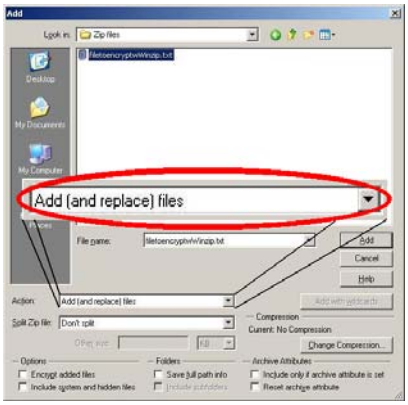
Files within a WinZip encrypted archive are protected on a removable medium that contains only the encrypted archive.

Files within a WinZip encrypted archive are protected when the archive is attached to an email.

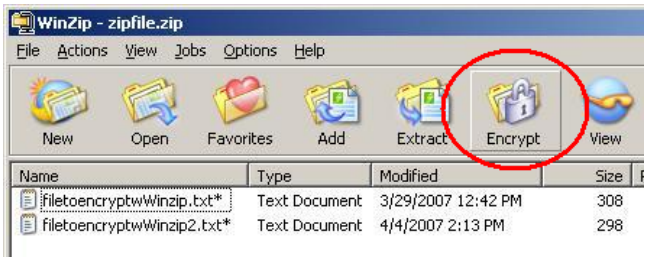
Any computer where the contents of a WinZip encrypted archive have been viewed or extracted will contain copies of the decrypted files in memory.

If using WinZip Version 10.0, use build 7245 to avoid a known vulnerability in earlier builds.

The recommendations in this pamphlet apply only to versions 10.0 and 11.0. Other versions should be examined for vulnerabilities before use.



Choose to add files to an archive rather than move files to an encrypted archive. When a file is moved to an archive, it appears that the original copy of the file is deleted, but the contents of the file still exist in the computer's memory. Adding files to an archive is safer because this leaves the original file intact, making it obvious to the user that the contents of the plain file still exist on the computer.



Encrypt the entire archive after all files have been added.

Use either 128-bit AES encryption or 256-bit AES encryption. Do not use Zip 2.0 compatible encryption.

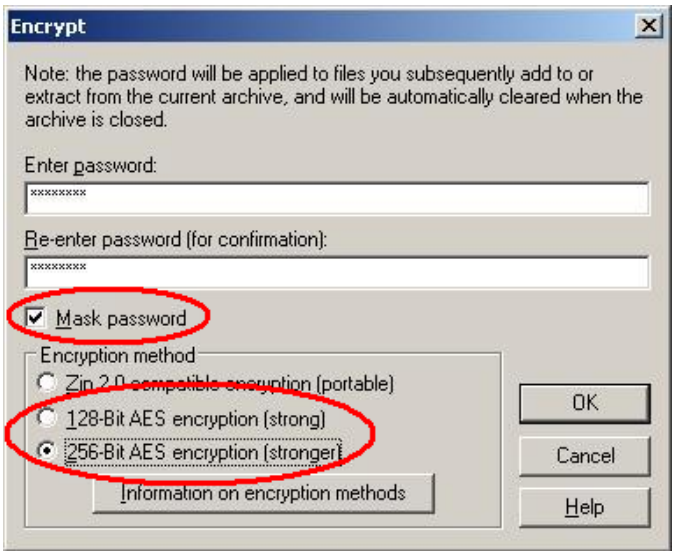
Use 256-bit AES encryption when encrypting a million files or more with the same password.

Refer to CNSSP-15 (www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf) for more guidance on choosing 128-bit or 256-bit key length.

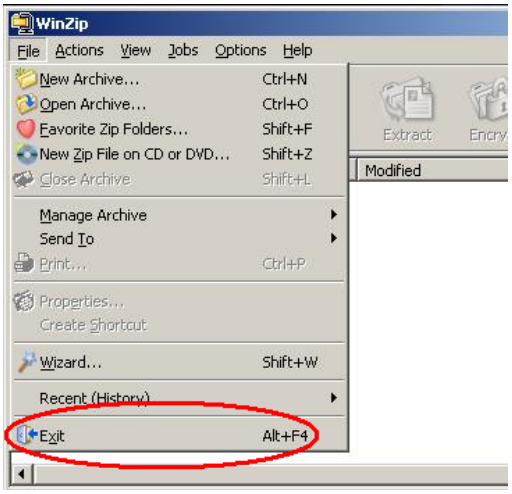
Reference “The 60 Minute Network Security Guide” (www.nsa.gov/snac/support/I33-011R-2006.pdf) for guidance on choosing strong passwords.

Choose to mask the password.

Implement a secure method for backing up passwords. WinZip does not provide a backup method for retrieving files from an encrypted archive when a password is forgotten.



This document outlined recommendations for WinZip users to assist in security their data. This document is not intended to replace your organization’s policy.



Close the WinZip program after closing an archive.